

## WO0116932

Publication Title:

DATA DISTRIBUTION SYSTEM

Abstract:

Abstract of WO0116932

A memory card (110) extracts a session key (Ks) by decoding data provided on a data bus (BS3) through a cellular network from a server. Encryption means (1406) encrypts a public key KPcard (1) of the memory card (110) based on the session key Ks and sends it to the server over the data bus (BS3). A register (1500) stores decrypted data, such as a license ID and a user ID, and a memory (1412) stores content data ([Dc]Kc) encrypted by the license key (Kc) and supplied over the data bus (BS3).

Data supplied from the esp@cenet database - Worldwide

-----  
Courtesy of <http://v3.espacenet.com>

(19) 世界知的所有権機関  
国際事務局(43) 国際公開日  
2001年3月8日 (08.03.2001)

PCT

(10) 国際公開番号  
WO 01/16932 A1(51) 国際特許分類<sup>7</sup>: G10K 15/02,  
G06F 15/00, 17/60, H04L 9/08, 9/10, G06K 19/00, H04H  
1/00, H04M 3/42, 3/493, 11/08, G10L 19/00, G06F 13/00,  
H04L 12/22, 12/58

(21) 国際出願番号: PCT/JP00/05770

(22) 国際出願日: 2000年8月25日 (25.08.2000)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:  
特願平11/241747 1999年8月27日 (27.08.1999) JP  
特願平11/345229 1999年12月3日 (03.12.1999) JP(71) 出願人 (米国を除く全ての指定国について): 富士通  
株式会社 (FUJITSU LIMITED) [JP/JP]; 〒211-8588 神奈川県川崎市中原区上小田中4丁目1番1号 Kanagawa  
(JP). 株式会社日立製作所 (HITACHI, LTD.) [JP/JP];  
〒101-8010 東京都千代田区神田駿河台四丁目6番地  
Tokyo (JP). 日本コロムビア株式会社 (NIPPON CO-  
LUMBIA CO., LTD.) [JP/JP]; 〒107-8011 東京都港区  
赤坂四丁目14番14号 Tokyo (JP). 三洋電機株式会社  
(SANYO ELECTRIC CO., LTD.) [JP/JP]; 〒570-8677  
大阪府守口市京阪本通2丁目5番5号 Osaka (JP).

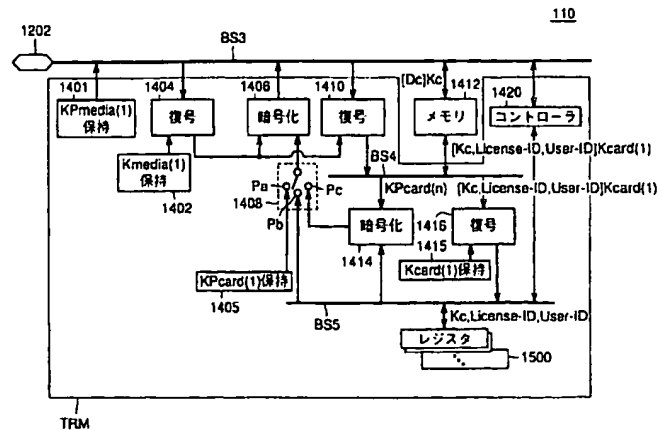
(72) 発明者; および

(75) 発明者/出願人 (米国についてのみ): 畑中正行  
(HATANAKA, Masayuki) [JP/JP]. 蒲田 順 (KA-  
MADA, Jun) [JP/JP]. 畠山卓久 (HATAKEYAMA,  
Takahisa) [JP/JP]. 長谷部高行 (HASEBE, Takayuki)  
[JP/JP]. 小谷誠剛 (KOTANI, Seigou) [JP/JP]. 古田茂  
樹 (FURUTA, Shigeki) [JP/JP]; 〒211-8588 神奈川  
県川崎市中原区上小田中4丁目1番1号 富士通株  
式会社内 Kanagawa (JP). 木下泰三 (KINOSHITA,  
Taizou) [JP/JP]; 〒187-8588 東京都小平市上水本  
町五丁目20番1号 株式会社日立製作所 半導体グ

[続葉有]

(54) Title: DATA DISTRIBUTION SYSTEM

(54) 発明の名称: データ配信システム



1402...HOLD Kmedia(1)	1412...MEMORY
1404...DECRYPT	1414...ENCRYPT
1405...HOLD Kpcard(1)	1415...HOLD Kpcard(1)
1406...ENCRYPT	1416...DECRYPT
1410...HOLD Kmedia(1)	1420...CONTROLLER
1410...DECRYPT	1500...REGISTER

(57) Abstract: A memory card (110) extracts a session key (Ks) by decoding data provided on a data bus (BS3) through a cellular network from a server. Encryption means (1406) encrypts a public key Kpcard (1) of the memory card (110) based on the session key Ks and sends it to the server over the data bus (BS3). A register (1500) stores decrypted data, such as a license ID and a user ID, and a memory (1412) stores content data ([Dc]Kc) encrypted by the license key (Kc) and supplied over the data bus (BS3).

[続葉有]



ループ内 Tokyo (JP). 穴澤健明 (ANAZAWA, Takeaki) [JP/JP]; 〒107-8011 東京都港区赤坂四丁目14番14号 日本コロムビア株式会社内 Tokyo (JP). 日置敏昭 (HIOKI, Toshiaki) [JP/JP]. 金森美和 (KANAMORI, Miwa) [JP/JP]. 堀 吉宏 (HORI, Yoshihiro) [JP/JP]; 〒570-8677 大阪府守口市京阪本通2丁目5番5号 三洋電機株式会社内 Osaka (JP).

(74) 代理人: 深見久郎, 外 (FUKAMI, Hisao et al.); 〒530-0054 大阪府大阪市北区南森町2丁目1番29号 住友銀行南森町ビル Osaka (JP).

(81) 指定国 (国内): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL,

PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) 指定国 (広域): ARIPO 特許 (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), ユーラシア特許 (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ特許 (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI 特許 (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:

— 国際調査報告書

2文字コード及び他の略語については、定期発行される各PCTガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

---

(57) 要約:

メモ리카ード110は、サーバから携帯電話網を介してデータベースBS3に与えられるデータから、復号処理をすることによりセッションキーKsを抽出する。暗号化処理部1406は、セッションキーKsに基づいて、メモ리카ード110の公開暗号化鍵Kpcard(1)を暗号化してデータベースBS3を介してサーバに与える。レジスタ1500は、復号されたライセンスID、ユーザID等のデータをサーバから受けとって格納し、メモリ1412は、データベースBS3からライセンスキーKcにより暗号化されている暗号化コンテンツデータ[Dc]Kcを受けて格納する。

## 明細書

## データ配信システム

## 5 技術分野

本発明は、携帯電話等の端末に対して情報を配送するためのデータ配信システムに関し、より特定のには、コピーされた情報に対する著作権保護を可能とするデータ配信システムに関するものである。

## 10 背景技術

近年、インターネット等の情報通信網等の進歩により、携帯電話等を用いた個人向け端末により、各ユーザが容易にネットワーク情報にアクセスすることが可能となっている。

このような情報通信においてはデジタル信号により情報が伝送される。したがって、たとえば上述のような情報通信網において伝送された音楽や映像情報を各個人ユーザがコピーした場合でも、そのようなコピーによる音質や画質の劣化をほとんど生じさせることなく、情報のコピーを行なうことが可能である。

したがって、このような情報通信網上において、音楽情報や画像情報等の著作権の存在する創作物が伝達される場合、適切な著作権保護のための方策が取られていないと、著しく著作権者の権利が侵害されてしまうおそれがある。

一方で、著作権保護の目的を最優先して、急拡大するデジタル情報通信網を介して著作物データの配信を行なうことができないとすると、基本的には、著作物の複製に際して一定の著作権料を徴収することが可能な著作権者にとっても、かえって不利益となる。

ここで、上述のようなデジタル情報通信網を介した配信ではなく、デジタル情報を記録した記録媒体を例にとりて考えてみると、通常販売されている音楽情報を記録したCD（コンパクトディスク）については、CDから光磁気ディスク（MD等）への音楽データのコピーは、当該コピーした音楽を個人的な使用に止める限り原則的には自由に行なうことができる。ただし、デジタル録音等を行な

う個人ユーザは、デジタル録音機器自体やMD等の媒体の代金のうちの一定額を間接的に著作権者に対して補償金として支払うことになっている。

- しかも、CDからMDへデジタル信号である音楽情報をコピーした場合、これらの情報がコピー劣化のほとんどないデジタル情報であることに鑑み、1つのMDからさらに他のMDに音楽データをデジタル情報としてコピーすることは、著作権者保護のために機器の構成上できないようになっている。

すなわち、現状においては、デジタル記録媒体であるCDからMDへのコピーは、親から子へのコピーは自由に行なうことができるものの、記録可能なMDからMDへのコピーを行なうことはできない。

- そのような事情からも、音楽データや画像データをデジタル情報通信網を通じて公衆に配信することは、それ自体が著作権者の公衆送信権による制限を受ける行為であるから、著作権保護のための十分な方策が講じられる必要がある。

- この場合、情報通信網を通じて公衆に送信される著作物データを、本来受信する権限のないユーザが受信することを防止する必要があるのはもちろんのこと、仮に権限を有するユーザが受信を行なった場合でも、一度受信された著作物が、さらに勝手に複製されることを防止することも必要となる。

#### 発明の開示

- 本発明の目的は、情報通信網、たとえば携帯電話等の情報通信網を介して著作物データを配信する場合に、正当なアクセス権を有するユーザのみがこのような情報を受信することが可能な情報配信システムを提供することである。

この発明の他の目的は、配信された著作物データが、著作権者の許可なく複製されることを防止することが可能な情報配信システムを提供することである。

- 係る目的を達成するために本願発明に係るデータ配信システムは、コンテンツデータ供給装置から、暗号化コンテンツデータを複数のユーザの各端末に配信するためのデータ配信システムである。

コンテンツデータ供給装置は、第1のインタフェース部と、第1のセッションキー発生部と、セッションキー暗号化部と、セッションキー復号部と、第1のライセンスデータ暗号化処理部と、第2のライセンスデータ暗号化処理部とを備え

る。

第1のインタフェース部は、外部との間でデータを授受する。

第1のセッションキー発生部は、暗号化コンテンツデータの通信ごとに更新される第1の共通鍵を生成する。セッションキー暗号化部は、ユーザの端末に対応して予め定められた第1の公開暗号化鍵により第1の共通鍵を暗号化して第1の  
5 インタフェース部に与える。セッションキー復号部は、第1の共通鍵により暗号化されて返信されるデータを復号する。

第1のライセンスデータ暗号化処理部は、暗号化コンテンツデータを復号するためのライセンスキーを、セッションキー復号部により復号されたデータを鍵データとして暗号化する。第2のライセンスデータ暗号化処理部は、第1のライ  
10 センスデータ暗号化処理部の出力を第2の共通鍵でさらに暗号化して第1のインタフェース部に与え配信する。

各端末は、第2のインタフェース部と、配信データ解読部とを備える。

第2のインタフェース部は、外部との間でデータを授受する。

配信データ解読部は、暗号化コンテンツデータを受けて格納する。配信データ  
15 解読部は、第1の鍵保持部と、第1の復号処理部と、第2の鍵保持部と、第1の暗号化処理部と、第2の復号処理部と、第1の記憶部と、第3の鍵保持部と、第3の復号処理部とを備える。

第1の鍵保持部は、第1の公開暗号化鍵によって暗号化されたデータを復号化  
20 するための第1の秘密復号鍵を保持する第1の復号処理部は、第1の公開暗号化鍵によって暗号化された第1の共通鍵を受けて、復号処理する。

第2の鍵保持部は、第2の公開暗号化鍵を保持する。第1の暗号化処理部は、第2の公開暗号化鍵を、第1の共通鍵に基づいて暗号化し、第2のインタフェース部に出力する。

第2の復号処理部は、第2のライセンスデータ暗号化処理部からの暗号化され  
25 たライセンスキーを受け、第2の共通鍵に基づいて復号化する。

第1の記憶部は、ライセンスキーに基づいて復号できる前記暗号化コンテンツデータを格納する。

第3の鍵保持部は、第2の公開暗号化鍵によって暗号化されたデータを復号化

するための第2の秘密復号鍵を保持する。第3の復号処理部は、第2の復号処理部での復号結果に基づいて、第2の秘密復号鍵によりライセンスキーを復号するためのを備える。

5 この発明のさらに他の局面に従うと、コンテンツデータ供給装置から、暗号化コンテンツデータと暗号化データを復号するためのライセンスキーとのうちの少なくとも1つを複数のユーザの各端末に配信するためのデータ配信システムである。

10 コンテンツデータ供給装置は、第1のインタフェース部と、第1のセッションキー発生部と、セッションキー暗号化処理部と、セッションキー復号部と、第1のライセンスデータ暗号化処理部と、第2のライセンス暗号化処理部とを備える。

第1のインタフェース部は、外部との間でデータを授受する。

15 第1のセッションキー発生部は、暗号化コンテンツデータの通信ごとに更新される第1の共通鍵を生成する。セッションキー暗号化処理部は、ユーザの端末に対応して予め定められた第1の公開暗号化鍵により第1の共通鍵を暗号化して第1のインタフェース部に与える。セッションキー復号部は、第1の共通鍵により暗号化されて返信される第2の共通鍵と第2の公開暗号化鍵を復号し抽出する。

20 第1のライセンスデータ暗号化処理部は、暗号化コンテンツデータを復号するためのライセンスキーを、セッションキー復号部により復号された第2の公開暗号化鍵により暗号化する。第2のライセンス暗号化処理部は、第1のライセンスデータ暗号化処理部の出力を第2の共通鍵でさらに暗号化して第1のインタフェース部に与え配信する。

各端末は、第2のインタフェース部と、配信データ解読部とを備える。

第2のインタフェース部は、外部との間でデータを授受する。

25 配信データ解読部は、暗号化コンテンツデータおよびライセンスキーを受けて格納する。

配信データ解読部は、第1の鍵保持部と、第1の復号処理部と、第2の鍵保持部と、第2のセッションキー発生部と、第1の暗号化処理部と、第2の復号処理部と、記憶部と、第3の鍵保持部と、第3の復号処理部と、第1の認証データ保

持部とを備える。

第1の鍵保持部は、第1の公開暗号化鍵によって暗号化されたデータを復号化するための第1の秘密復号鍵を保持する。第1の復号処理部は、第1の公開暗号化鍵によって暗号化された第1の共通鍵を受けて、復号処理する。

- 5 第2の鍵保持部は、第2の公開暗号化鍵を保持する。第2のセッションキー発生部は、第2の共通鍵を生成する。

- 第1の暗号化処理部は、第2の公開暗号化鍵と第2の共通鍵を、第1の共通鍵に基づいて暗号化し、第2のインタフェース部に出力する。第2の復号処理部は、第2のライセンスデータ暗号化処理部からの暗号化されたライセンスキーを受け、第2の共通鍵に基づいて復号する。記憶部は、ライセンスキーにて復号可能な暗号化コンテンツデータを格納する。
- 10

- 第3の鍵保持部は、第2の公開暗号化鍵によって暗号化されたデータを復号化するための第2の秘密復号鍵を保持する。第3の復号処理部は、第2の復号処理部での復号結果に基づいて、第2の秘密復号鍵によりライセンスキーを復号し抽出する。第1の認証データ保持部は、第1の公開暗号化鍵を少なくとも含む第1の認証データを公開認証鍵により復号できるように暗号化して保持し外部に出力可能である。
- 15

- コンテンツデータ供給装置は、公開認証鍵により復号でき、かつ外部から与えられる第1の認証データを復号して抽出するための第1の認証復号処理部と、第1の認証復号処理部により抽出された第1の認証データに基づいて認証処理を行ない、少なくともライセンスキーを配信するか否かを判断する配信制御部をさらに含む。
- 20

- したがって、本発明によれば、正規のユーザのみがコンテンツデータを受信してメモリ中に格納することが可能となる。しかも、1度メモリカード中に格納されたデータを、他人にコピーさせる場合は、当該他人が再生可能な状態でデータを移植するためには、送信元においては、データの再生が不能となってしまう構成となっているので、無制限なコピーにより著作権が不当な不利益を被るのを防止することが可能となる。
- 25

この発明の他の利点は、認証された端末にのみライセンスキーが配信されるの



で、著作権の保護が一層強化されることである。

この発明のさらに他の利点は、ユーザが配信キャリアを介してではなく、コンテンツデータ販売機により暗号化コンテンツデータを購入することができるので、ユーザの利便性が一層向上することである。

5

#### 図面の簡単な説明

図 1 は、本発明の情報配信システムの全体構成を概略的に説明するための概念図である。

10 図 2 は、図 1 に示した情報配信システムにおいて使用される通信のためのキーデータ（鍵データ）等の特性をまとめて説明する図である。

図 3 は、図 1 に示した配信サーバ 10 の構成を示す概略ブロック図である。

図 4 は、図 1 に示した携帯電話機 100 の構成を説明するための概略ブロック図である。

15 図 5 は、図 4 に示したメモ리카ード 110 の構成を説明するための概略ブロック図である。

図 6 は、図 1 および図 3 ～図 5 で説明したデータ配信システムにおける配信モードを説明するための第 1 のフローチャートである。

図 7 は、図 1 および図 3 ～図 5 で説明したデータ配信システムにおける配信モードを説明するための第 2 のフローチャートである。

20 図 8 は、携帯電話機 100 内においてコンテンツデータを再生し、音楽として外部に出力するための再生処理を説明するフローチャートである。

図 9 は、2つのメモ리카ード間において、コンテンツデータおよびキーデータ等の移動または複製を行なう処理を説明するための第 1 のフローチャートである。

25 図 10 は、2つのメモ리카ード間において、コンテンツデータおよびキーデータ等の移動または複製を行なう処理を説明するための第 2 のフローチャートである。

図 11 は、実施の形態 2 のメモ리카ード 120 に対応した音楽サーバ 31 の構成を示す概略ブロック図である。

図12は、実施の形態2における携帯電話機101の構成を説明するための概略ブロック図である。

図13は、本発明の実施の形態2のメモリカード120の構成を説明するための概略ブロック図である。

- 5 図14は、図13で説明したメモリカード120を用いた配信モードを説明するための第1のフローチャートである。

図15は、図13で説明したメモリカード120を用いた配信モードを説明するための第2のフローチャートである。

- 10 図16は、携帯電話機101内においてコンテンツデータを再生し、音楽として外部に出力するための再生処理を説明する第1のフローチャートである。

図17は、携帯電話機101内においてコンテンツデータを再生し、音楽として外部に出力するための再生処理を説明する第2のフローチャートである。

図18は、2つのメモリカード間でコンテンツデータおよびキーデータ等の移動または複製を行なう処理を説明するための第1のフローチャートである。

- 15 図19は、2つのメモリカード間でコンテンツデータおよびキーデータ等の移動または複製を行なう処理を説明するための第2のフローチャートである。

図20は、実施の形態3のデータ配信システムの構成を説明するための概念図である。

- 20 図21は、実施の形態3のコンテンツデータ販売機2000の構成を示す概略ブロック図である。

図22は、図20および図21で説明したデータ配信システムにおける配信モードを説明するための第1のフローチャートである。

図23は、図20および図21で説明したデータ配信システムにおける配信モードを説明するための第2のフローチャートである。

- 25 図24は、実施の形態3の変形例のコンテンツデータ販売機2001の構成を示す概念図である。

図25は、実施の形態3の変形例のデータ配信システムにおける配信モードを説明するための第1のフローチャートである。

図26は、実施の形態3の変形例のデータ配信システムにおける配信モードを

説明するための第2のフローチャートである。

図27は、実施の形態4のコンテンツデータ販売機3000の構成を説明するための概略ブロック図である。

5 図28は、図27で説明したデータ配信システムにおける配信モードを説明するための第1のフローチャートである。

図29は、図27で説明したデータ配信システムにおける配信モードを説明するための第2のフローチャートである。

図30は、実施の形態4の変形例のデータ配信システムにおける配信モードを説明するための第1のフローチャートである。

10 図31は、実施の形態4の変形例のデータ配信システムにおける配信モードを説明するための第2のフローチャートである。

図32は、実施の形態5における携帯電話機105の構成を説明するための概略ブロック図である。

15 図33は、実施の形態5のメモリカード140に対応した配信サーバ12の構成を示す概略ブロック図である。

図34は、本発明の実施の形態5のメモリカード140の構成を説明するための概略ブロック図である。

図35は、メモリカード140を用いた配信モードを説明するための第1のフローチャートである。

20 図36は、メモリカード140を用いた配信モードを説明するための第2のフローチャートである。

図37は、メモリカード140に保持された暗号化コンテンツデータから、音楽として外部に出力するための再生処理を説明する第1のフローチャートである。

25 図38は、メモリカード140に保持された暗号化コンテンツデータから、音楽として外部に出力するための再生処理を説明する第2のフローチャートである。

図39は、2つのメモリカード間において、コンテンツデータおよびキーデータ等の移動または複製を行なう処理を説明するための第1のフローチャートであ

る。

図40は、2つのメモリカード間において、コンテンツデータおよびキーデータ等の移動または複製を行なう処理を説明するための第2のフローチャートである。

- 5 図41は、本発明の実施の形態6のコンテンツデータ販売機3010の構成を示す概略ブロック図である。

図42は、コンテンツデータ販売機3010を用いたデータ配信システムにおける配信モードを説明するための第1のフローチャートである。

- 10 図43は、コンテンツデータ販売機3010を用いたデータ配信システムにおける配信モードを説明するための第2のフローチャートである。

図44は、実施の形態7における携帯電話機107の構成を説明するための概略ブロック図である。

図45は、実施の形態7の携帯電話機107に対応した配信サーバ13の構成を示す概略ブロック図である。

- 15 図46は、配信サーバ12と携帯電話機107を用いた配信モードを説明するための第1のフローチャートである。

図47は、配信サーバ12と携帯電話機107を用いた配信モードを説明するための第2のフローチャートである。

- 20 図48は、メモリカード140に保持された暗号化コンテンツデータから、音楽として外部に出力するための再生処理を説明する第1のフローチャートである。

図49は、メモリカード140に保持された暗号化コンテンツデータから、音楽として外部に出力するための再生処理を説明する第2のフローチャートである。

- 25 図50は、実施の形態7において、2つのメモリカード間において、コンテンツデータおよびキーデータ等の移動または複製を行なう処理を説明するための第1のフローチャートである。

図51は、実施の形態7において、2つのメモリカード間において、コンテンツデータおよびキーデータ等の移動または複製を行なう処理を説明するための第

2のフローチャートである。

図52は、本発明の実施の形態8のコンテンツデータ販売機3020の構成を示す概略ブロック図である。

5 図53は、コンテンツデータ販売機3020を用いたデータ配信システムにおける配信モードを説明するための第1のフローチャートである。

図54は、コンテンツデータ販売機3020を用いたデータ配信システムにおける配信モードを説明するための第2のフローチャートである。

図55は、メモリカード140の端子1202部分の構成を説明する概略ブロック図である。

10 図56は、メモリカード140の端子1202部分の構成の変形例を説明するための概略ブロック図である。

発明を実施するための最良の形態

以下、本発明の実施例を図面とともに説明する。

15 [実施例1]

[システムの全体構成]

図1は、本発明の情報配信システムの全体構成を概略的に説明するための概念図である。

20 なお、以下では携帯電話網を介して、音楽データを各ユーザに配信するデータ配信システムの構成を例にとって説明するが、以下の説明で明らかとなるように、本発明はこのような場合に限定されることなく、他の著作物データ、たとえば画像データ等の著作物データを、他の情報通信網を介して配信する場合にも適用することが可能なものである。

25 図1を参照して、著作権の存在する音楽情報を管理する配信サーバ10は、所定の暗号方式により音楽データ（以下コンテンツデータとも呼ぶ）を暗号化したうえで、情報を配信するための配信キャリア20である携帯電話会社に、このような暗号化データを与える。一方、認証サーバ12は、音楽データの配信を求めてアクセスしてきた機器が正規の機器であるか否かの認証を行なう。

配信キャリア20は、自己の携帯電話網を通じて、各ユーザからの配信要求

(配信リクエスト)を配信サーバ10に中継する。配信サーバ10は、配線リクエストがあると、認証サーバ12により正規の機器からのアクセスであることを確認し、要求されたコンテンツデータをさらに暗号化したうえで、配信キャリア20の携帯電話網を介して、各ユーザの携帯電話機に対して配信する。

5 図1においては、たとえば携帯電話ユーザ1の携帯電話機100には、携帯電話機100により受信された暗号化コンテンツデータを受取って、上記送信にあたって行なわれた暗号化については復号化したうえで、携帯電話機100中の音楽再生部(図示せず)に与えるための着脱可能なメモリカード110に格納する構成となっている。

10 さらに、たとえばユーザ1は、携帯電話機100に接続したヘッドホン130等を介してこのようなコンテンツデータを再生した音楽を聴取することが可能である。

以下では、このような配信サーバ10と認証サーバ12と配信キャリア20とを併せて、音楽サーバ30と総称することにする。

15 また、このような音楽サーバ30から、各携帯電話端末等にコンテンツデータを伝送する処理を「配信」と称することとする。

このような構成とすることで、まず、正規のメモリカードであるメモリカード110を購入していない正規のユーザでないものは、音楽サーバ30からの配信データを受取って再生することが困難な構成となる。

20 しかも、配信キャリア20において、たとえば1曲分のコンテンツデータを配信するたびにその度数を計数しておくことで、ユーザがコンテンツデータを受信(ダウンロード)するたびに発生する著作権料を、配信キャリア20が携帯電話の通話料金として徴収することとすれば、著作権者が著作権料を確保することが容易となる。

25 しかも、このようなコンテンツデータの配信は、携帯電話網というクローズドなシステムを介して行なわれるため、インターネット等のオープンなシステムに比べて、著作権保護の対策を講じやすいという利点がある。

このとき、たとえばメモリカード112を有するユーザ2が、自己の携帯電話機102により、音楽サーバ30から直接コンテンツデータの配信を受けること

は可能である。しかしながら、相当量の情報量を有するコンテンツデータ等をユーザ2が直接音楽サーバ30から受信することとすると、その受信のために比較的に長い時間を要してしまう場合がある。このような場合、既に当該コンテンツデータの配信を受けているユーザ1から、そのコンテンツデータをコピーできることを可能としておけば、ユーザにとっての利便性が向上する。

しかしながら、著作権者の権利保護の観点からは、自由なコンテンツデータのコピーを放任することはシステム構成上許されない。

図1に示した例では、ユーザ1が受信したコンテンツデータを、コンテンツデータそのものおよび当該コンテンツデータを再生可能とするために必要な情報とともに、ユーザ2に対してコピーさせる場合をコンテンツデータの「移動」と呼ぶ。この場合、ユーザ1は、再生のために必要な情報（再生情報）ごとユーザ2にコピーさせるため、情報の移動を行なった後には、ユーザ1においてはコンテンツデータの再生を行なうことは不可能とする必要がある。ここで、コンテンツデータは所定の暗号化方式にしたがって暗号化された暗号化コンテンツデータとして配信され、「再生情報」とは、後に説明するように、上記所定の暗号化方式にしたがって暗号化コンテンツデータを復号可能な鍵（ライセンスキーとも称する）と、著作権保護に関わる情報であるライセンスIDデータやユーザIDデータ等のライセンス情報とを意味する。

これに対して、コンテンツデータのみを暗号化されたままの状態、ユーザ2にコピーさせることを音楽情報の「複製」と呼ぶこととする。

この場合、ユーザ2の端末には、このようなコンテンツデータを再生させるために必要な再生情報はコピーされない、ユーザ2は、暗号化コンテンツデータを得ただけでは、音楽を再生させることができない。したがって、ユーザ2が、このような音楽の再生を望む場合は、改めて音楽サーバ30からコンテンツデータの再生を可能とするための再生情報の配信を受ける必要がある。しかしながら、この場合は、再生を可能とするための情報の配信のみを受ければよい、ため、ユーザ2が直接音楽サーバ30からすべての配信を受ける場合に比べて、格段に短い通話時間で、音楽再生を可能とすることができる。

たとえば、携帯電話機100および102が、PHS（Personal Handy

Phone) である場合には、いわゆるトランシーバモードの通話が可能となっているので、このような機能を利用して、ユーザ1からユーザ2への一括した情報の移転（移動）や、暗号化したコンテンツデータのみの転送（複製）を行なうことが可能である。

- 5      図1に示したような構成においては、暗号化して配信されるコンテンツデータをユーザ側で再生可能とするためにシステム上必要とされるのは、第1には、通信における暗号化キー（鍵）を配送するための方式であり、さらに第2には、配信データを暗号化する方式そのものであり、さらに、第3には、このようにして配信されたデータの無断コピーを防止するためのデータ保護を実現する構成である。
- 10      る。

    [暗号／復号鍵の構成]

    図2は、図1に示した情報配信システムにおいて使用される通信のためのキーデータ（鍵データ）等の特性をまとめて説明するための図である。

- まず、図1に示した構成において、メモ리카ード100内のデータ処理を管理  
15      するための鍵としては、メモ리카ードという媒体の種類に固有であり、かつ、メモ리카ードの種類等を個別に特定するための情報を含む秘密復号鍵 $K_{media}(n)$ （ $n$ ：自然数）と、メモ리카ードごとに異なる公開暗号化鍵 $K_{Pcard}(n)$ と、公開暗号化鍵 $K_{Pcard}(n)$ により暗号化されたデータを復号するための秘密復号鍵 $K_{card}(n)$ とがある。

- 20      ここで、鍵 $K_{card}(n)$ や鍵 $K_{Pcard}(n)$ の表記中の自然数 $n$ は、各メモ리카ードを区別するための番号を表わす。

- すなわち、公開暗号化鍵 $K_{Pcard}(n)$ で暗号化されたデータは、各メモ  
    リカードごとに存在する秘密復号鍵 $K_{card}(n)$ で復号可能である。したが  
    って、メモ리카ードにおける配信データの授受にあたっては、基本的には、後に  
25      説明するように3つの暗号鍵 $K_{media}(n)$ 、 $K_{card}(n)$ 、 $K_{Pcard}(n)$ が用いられることになる。

    さらに、メモ리카ード外とメモ리카ード間でのデータの授受における秘密保持のための暗号鍵としては、各媒体に固有な公開暗号化鍵 $K_{Pmedia}(n)$ と、公開暗号化鍵 $K_{Pmedia}(n)$ により暗号化されたデータを復号化する



ための秘密復号鍵  $K_{media(n)}$  と、各通信ごと、たとえば、音楽サーバ 30 へのユーザのアクセスごとに音楽サーバ 30、携帯電話機 100 または 102 において生成される共通鍵  $K_s$  が用いられる。

5      ここで、共通鍵  $K_s$  は、たとえば、ユーザが音楽サーバ 30 に対して 1 回のアクセスを行なうごとに発生する構成として、1 回のアクセスである限り何曲の音楽情報についても同一の共通鍵が用いられる構成としてもよいし、また、たとえば、各曲目ごとにこの共通鍵を変更したうえでその都度ユーザに配信する構成としてもよい。

10      以下では、このような通信の単位あるいはアクセスの単位を「セッション」と呼ぶことにし、共通鍵  $K_s$  を「セッションキー」とも呼ぶことにする。

したがって、共通鍵  $K_s$  は各通信セッションに固有の値を有することになり、配信サーバや携帯電話機において管理される。

15      また、配信されるべきデータについては、まず、暗号化コンテンツデータを復号する鍵である  $K_c$ （以下、ライセンスキーと呼ぶ）があり、このライセンスキー  $K_c$  により暗号化コンテンツデータが復号化されるものとする。さらに、上述したライセンス情報として、当該コンテンツデータを特定できる管理コードや、再生を行なう回数の制限などの情報を含むライセンス ID データ  $License-ID$  等が存在する。一方、携帯電話は、受信者を識別するためのユーザ ID データ  $User-ID$  を保持している。

20      このような構成とすることで、ライセンス ID データに含まれる情報に応じて、著作権者側の著作権保護に関する制御を行なうことが可能であり、一方ユーザ ID データを用いることで、ユーザの個人情報の保護、たとえばユーザのアクセス履歴等が部外者から知ることができないように保護するといったような制御を行なうことが可能である。

25      配信データにおけるコンテンツデータ  $D_c$  は、上述のとおり、たとえば音楽データであり、このコンテンツデータをライセンスキー  $K_c$  で復号化可能なデータを、暗号化コンテンツデータ  $[D_c] K_c$  と呼ぶ。

ここで、 $[Y] X$  という表記は、データ  $Y$  を、キー（鍵） $X$  により復号可能な暗号に変換したデータであることを示している。なお、暗号化处理、復号処理で

用いられる鍵を、「キー」とも称することとする。

〔配信サーバ１０の構成〕

図３は、図１に示した配信サーバ１０の構成を示す概略ブロック図である。配信サーバ１０は、コンテンツデータ（音楽データ）を所定の方式に従って暗号化したデータや、ライセンスＩＤ等の配信情報を保持するための配信情報データベース３０４と、各ユーザごとにコンテンツデータへのアクセス回数等に従った課金情報を保持するための課金データベース３０２と、配信情報データベース３０４および課金データベース３０２からのデータをデータベースＢＳ１を介して受取り、所定の暗号化処理を行なうためのデータ処理部３１０と、通信網を介して、配信キャリア２０とデータ処理部３１０との間でデータ授受を行なうための通信装置３５０とを備える。

データ処理部３１０は、データベースＢＳ１上のデータに応じて、データ処理部３１０の動作を制御するための配信制御部３１２と、配信制御部３１２に制御されて、セッションキーＫｓを発生するためのセッションキー発生部３１４と、セッションキー発生部３１４より生成されたセッションキーＫｓを、公開暗号化鍵ＫＰｍｅｄｉａにより暗号化して、データベースＢＳ１に与えるための暗号化処理部３１６と、各ユーザの携帯電話機においてセッションキーＫｓにより暗号化されたうえで送信されたデータを通信装置３５０およびデータベースＢＳ１を介して受けて、復号処理を行なう復号処理部３１８と、復号処理部３１８により抽出された公開暗号化鍵ＫＰｃａｒｄ（ｎ）を用いて、ライセンスキーやライセンスＩＤ等のデータを配信制御部３１２に制御されて暗号化するための暗号化処理部３２０と、暗号化処理部３２０の出力を、さらにセッションキーＫｓにより暗号化して、データベースＢＳ１を介して通信装置３５０に与える暗号化処理部３２２とを含む。

〔端末（携帯電話機）の構成〕

図４は、図１に示した携帯電話機１００の構成を説明するための概略ブロック図である。

携帯電話機１００は、携帯電話網により無線伝送される信号を受信するためのアンテナ１１０２と、アンテナ１１０２からの信号を受けてベースバンド信号に

変換し、あるいは携帯電話機からのデータを変調してアンテナ 1102 に与えるための送受信部 1104 と、携帯電話機 100 の各部のデータ授受を行なうためのデータバス BS2 と、データバス BS2 を介して携帯電話機 100 の動作を制御するためのコントローラ 1106 と、受信者を識別するためのユーザ ID データ User ID を保持するユーザ ID 保持部 1107 と、外部からの指示を携帯電話機 100 に与えるためのタッチキー部 1108 と、コントローラ 1106 等から出力される情報をユーザに視覚情報として与えるためのディスプレイ 1110 と、通常の通話動作において、データバス BS2 を介して与えられる受信データに基づいて音声を再生するための音声再生部 1112 と、外部との間でデータの授受を行なうためのコネクタ 1120 と、コネクタ 1120 からのデータをデータバス BS2 に与え得る信号に変換し、または、データバス BS2 からのデータをコネクタ 1120 に与え得る信号に変換するための外部インタフェース部 1122 とを備える。

ここで、ユーザ ID データは、たとえばユーザの電話番号等のデータを含む。

15 携帯電話機 100 は、さらに、音楽サーバ 30 からのコンテンツデータを復号化処理するための着脱可能なメモリカード 110 と、メモリカード 110 とデータバス BS2 との間のデータの授受を制御するためのメモリインタフェース 1200 と、メモリカード 110 と携帯電話機の他の部分とのデータ授受にあたり、データバス BS2 上においてやり取りされるデータを暗号化するためのセッションキー Ks を乱数等により発生するセッションキー発生部 1502 と、セッションキー発生部 1502 により生成されたセッションキーを暗号化して、データバス BS2 に与えるための暗号化処理部 1504 と、セッションキー発生部 1502 において生成された、データバス BS2 上のデータをセッションキー Ks により復号して出力する復号処理部 1506 と、復号処理部 1506 の出力を受けて、音楽信号を再生するための音楽再生部 1508 と、音楽再生部 1508 の出力と音声再生部 1112 の出力とを受けて、動作モードに応じて選択的に出力するための混合部 1510 と、混合部 1510 の出力を受けて、外部に出力するためのアナログ信号に変換するデジタルアナログ変換部 1512 と、デジタルアナログ変換部 1512 の出力を受けて、ヘッドホン 130 と接続するための接続端

子1514とを含む。

なお、説明の簡素化のため本発明のコンテンツデータの配信に関わるブロックのみを記載し、携帯電話機が本来備えている通話機能に関するブロックについては、一部割愛されている。

5      [メモ리카ードの構成]

図5は、図4に示したメモ리카ード110の構成を説明するための概略ブロック図である。

以下では、端末100に装着されるメモ리카ード110の公開暗号化鍵K P m e d i a と、端末102に装着されるメモ리카ード112の公開暗号化鍵K P m e d i a とを区別して、それぞれ、メモ리카ード110に対するものを公開暗号化鍵K P m e d i a (1) と、メモ리카ード112に対するものを公開暗号化鍵K P m e d i a (2) と称することにする。

また、これに対応して、公開暗号化鍵K P m e d i a (1) で暗号化されたデータを復号可能であって、これとは非対称な秘密復号鍵を秘密復号鍵K m e d i a (1) と称し、公開暗号化鍵K P m e d i a (2) で暗号化されたデータを復号可能であって、これとは非対称な秘密復号鍵を秘密復号鍵K m e d i a (2) と称することにする。

このように、媒体固有の公開暗号化鍵を区別することにより、以下の説明で明らかとなるように、メモ리카ードに複数の種類が存在する場合や、より一般的に、メモ리카ード以外の媒体がシステムのオプションとして存在する場合にも、対応することが可能となる。

メモ리카ード110は、メモリインタフェース1200との間で信号を端子1202を介して授受するデータバスB S 3と、公開暗号化鍵K P m e d i a (1) の値を保持し、データバスB S 3に公開暗号化鍵K P m e d i a (1) を出力するためのK P m e d i a (1) 保持部1401と、メモ리카ード110に対応する秘密復号鍵K m e d i a (1) を保持するためのK m e d i a (1) 保持部1402と、データバスB S 3にメモリインタフェース1200から与えられるデータから、秘密復号鍵K m e d i a (1) により復号処理をすることにより、セッションキーK s を抽出する復号処理部1404と、公開暗号化鍵K P c

ard (1) を保持するための K P c a r d (1) 保持部 1 4 0 5 と、復号処理部 1 4 0 4 により抽出されたセッションキー K s に基づいて、切換スイッチ 1 4 0 8 からの出力を暗号化してデータベース B S 3 に与えるための暗号化処理部 1 4 0 6 と、データベース B S 3 上のデータを復号処理部 1 4 0 4 により抽出されたセッションキー K s により復号処理してデータベース B S 4 に与えるための復号処理部 1 4 1 0 と、データベース B S 4 からメモ리카ードごとに異なる公開暗号化鍵 K P c a r d (n) で暗号化されているライセンスキー K c、ライセンス I D 等のデータを格納し、データベース B S 3 からライセンスキー K c により暗号化されている暗号化コンテンツデータ [D c] K c を受けて格納するためのメモリ 1 4 1 2 とを備える。

切換えスイッチ 1 4 0 8 は、接点 P a、P b、P c を有し、接点 P a には K P c a r d (1) 保持部 1 4 0 5 からの公開暗号化鍵 K P c a r d (1) が、接点 P b にはデータベース B S 5 が、接点 P c には暗号化処理部 1 4 1 4 の出力が与えられる。切換えスイッチ 1 4 0 8 は、それぞれ、接点 P a、P b、P c に与えられる信号を、動作モードが、「配信モード」、「再生モード」、「移動モード」のいずれであるかに応じて、選択的に暗号化処理部 1 4 0 6 に与える。

メモ리카ード 1 1 0 は、さらに、秘密復号鍵 K c a r d (1) の値を保持するための K c a r d (1) 保持部 1 4 1 5 と、公開暗号化鍵 K P c a r d (1) により暗号化されており、かつ、メモリ 1 4 1 2 から読み出されたライセンスキー K c、ライセンス I D 等 ([K c, L i c e n s e] K c a r d (1)) を、復号処理してデータベース B S 5 に与える復号処理部 1 4 1 6 と、データの移動処理等において、相手先のメモ리카ードの公開暗号化鍵 K P c a r d (n) を復号処理部 1 4 1 0 から受けて、この相手方の公開暗号化鍵 K P c a r d (n) に基づいて、データベース B S 5 上に出力されているライセンスキー K c、ライセンス I D 等を暗号化したうえで、切換スイッチ 1 4 0 8 に出力するための暗号化処理部 1 4 1 4 と、データベース B S 3 を介して外部とデータの授受を行い、データベース B S 5 との間でライセンス I D データ等を受けて、メモ리카ード 1 1 0 の動作を制御するためのコントローラ 1 4 2 0 と、データベース B S 5 との間でライセンス I D データ等のデータの授受が可能なレジスタ 1 5 0 0 とを備える。

なお、図5において実線で囲んだ領域は、メモ리카ード110内において、外部からの不当な開封処理等が行なわれると、内部データの消去や内部回路の破壊により、第三者に対してその領域内に存在する回路内のデータ等の読み出しを不能化するためのモジュールTRMに組込まれているものとする。

- 5       このようなモジュールは、一般にはタンパーレジスタンスモジュール (Tamper Resistance Module) と呼ばれる。

もちろん、メモリ1412も含めて、モジュールTRM内に組み込まれる構成としてもよい。しかしながら、図5に示したような構成とすることで、メモリ1412中に保持されているデータは、いずれも暗号化されているデータであるため、第三者はこのメモリ1412中のデータのみでは、音楽を再生することは不可能であり、かつ高価なタンパーレジスタンスモジュール内にメモリ1412を設ける必要がないので、製造コストが低減されるという利点がある。

図6および図7は、図1および図3～図5で説明したデータ配信システムにおける配信動作を説明するための第1および第2のフローチャートである。

- 15       図6および図7においては、ユーザ1が、メモ리카ード110を用いることで、音楽サーバ30から音楽データの配信を受ける場合の動作を説明している。

まず、ユーザ1の携帯電話機100から、ユーザによりタッチキー1108のキーボタンの操作等によって、配信リクエストがなされる (ステップS100)。

- 20       メモ리카ード110においては、この配信リクエストに応じて、K P m e d i a (1) 保持部1401から、公開暗号化鍵K P m e d i a (1) を音楽サーバ30に対して送信する (ステップS102)。

音楽サーバ30では、メモ리카ード110から転送された配信リクエストならびに公開暗号化鍵K P m e d i a (1) を受信すると (ステップS104)、受信した公開暗号化鍵K P m e d i a (1) に基づいて、認証サーバ12に対して照会を行ない、正規メモ리카ードからのアクセスの場合は次の処理に移行し (ステップS106)、正規メモ리카ードでない場合には、処理を終了する (ステップS154)。

照会の結果、正規メモ리카ードであることが確認されると、音楽サーバ30で

は、セッションキー発生部314が、セッションキーKsを生成する。さらに、音楽サーバ30内の暗号化処理部316が、受信した公開暗号化鍵K P m e d i a (1)により、このセッションキーKsを暗号化して暗号化セッションキー[Ks] K m e d i a (1)を生成する(ステップS108)。

- 5 続いて、音楽サーバ30は、暗号化セッションキー[Ks] K m e d i a (1)をデータベースBS1に与える。通信装置350は、暗号化処理部316からの暗号化セッションキー[Ks] K m e d i a (1)を、通信網を通じて、携帯電話機100のメモ리카ード110に対して送信する(ステップS110)。

- 10 携帯電話機100が、暗号化セッションキー[Ks] K m e d i a (1)を受信すると(ステップS112)、メモ리카ード110においては、メモリインタフェース1200を介して、データベースBS3に与えられた受信データを、復号処理部1404が、秘密復号鍵K m e d i a (1)により復号処理することにより、セッションキーKsを復号し抽出する(ステップS114)。

- 15 続いて、配信動作においては、切換スイッチ1408は、接点Paが閉じる状態が選択されているので、暗号化処理部1406は、接点Paを介してK P c a r d (1)保持部1405から与えられる公開暗号化鍵K P c a r d (1)(メモ리카ード110に対する公開暗号化鍵)を、セッションキーKsにより暗号化し(ステップS116)、データ[K P c a r d (1)] Ksを生成する(ステップS118)。

- 20 携帯電話機100は、暗号化処理部1406により暗号化されたデータ[K P c a r d (1)] Ksを音楽サーバ30に対して送信する(ステップS120)。

- 25 音楽サーバ30では、通信装置350によりデータ[K P c a r d (1)] Ksが受信され(ステップS122)、データベースBS1に与えられたデータ[K P c a r d (1)] Ksを復号処理部318が、セッションキーKsにより復号処理して、公開暗号化鍵K P c a r d (1)を復号抽出する(ステップS124)。

続いて、配信制御部312は、配信情報データベース304等に保持されているデータを元に、ライセンスIDデータ等を含むライセンス情報データL i c e

n s eを生成する（ステップS 1 2 6）。

さらに、音楽サーバ3 0は、暗号化コンテンツデータ [D c] K cを配信情報データベース3 0 4より取得して、通信装置3 5 0を介して、メモリカード1 1 0に送信する（ステップS 1 2 8）。

- 5 携帯電話機1 0 0がデータ [D c] K cを受信すると（ステップS 1 3 0）、メモリカード1 1 0においては、受信したデータ [D c] K cをそのままメモリ1 4 1 2に格納する（ステップS 1 3 2）。

- 一方、音楽サーバ3 0は、ライセンスキーK cを配信情報データベース3 0 4より取得し（ステップS 1 3 4）、暗号化処理部3 2 0は、配信制御部3 1 2からのライセンスキーK cとライセンス情報データL i c e n s eとを、復号処理部3 1 8より与えられた公開暗号化鍵K P c a r d (1)により暗号化処理する（ステップS 1 3 6）。

- 暗号化処理部3 2 2は、暗号化処理部3 2 0により暗号化されたデータ [K c、L i c e n s e] K c a r d (1)を受取って、さらにセッションキーK sにより暗号化したデータをデータバスB S 1に与える。通信装置3 5 0は、暗号化処理部3 2 2により暗号化されたデータ [ [K c、L i c e n s e] K c a r d (1) ] K sをメモリカード1 1 0に対して送信する。

- 携帯電話機1 0 0がデータ [ [K c、L i c e n s e] K c a r d (1) ] K sを受信すると（ステップS 1 4 2）、メモリカード1 1 0においては、復号処理部1 4 1 0がセッションキーK sにより復号処理を行ない、データ [K c、L i c e n s e] K c a r d (1)を抽出し、メモリ1 4 1 2に記録（格納）する（ステップS 1 4 6）。

- さらに、メモリカード1 1 0においては、コントローラ1 4 2 0により制御されて、復号処理部1 4 1 6が、メモリ1 4 1 2に格納されたデータ [K c、L i c e n s e] K c a r d (1)を復号し、復号されたライセンス情報データL i c e n s eを、レジスタ1 5 0 0に格納する（ステップ1 4 8）。

以上のような動作により、メモリカード自身が、セッションキーK sを送る側（音楽サーバ3 0）に、公開暗号化鍵K P m e d i a (1)を送信した上で、配信を受けることができ、メモリカード1 1 0が格納するコンテンツデータは再生



可能な状態となる。以下では、メモ리카ードが格納するコンテンツデータが再生可能な状態となっていることを、「メモ리카ード110は、状態SAにある」と呼ぶことにする。一方、メモ리카ードが格納するコンテンツデータが再生不可能な状態となっていることを、「メモ리카ード110は、状態SBにある」と呼ぶことにする。

さらに、メモ리카ード110から音楽サーバ30へは、配信受理が通知され、音楽サーバ30で配信受理を受信すると（ステップS150）、課金データベース302にユーザ1の課金データが格納され（ステップS152）、処理が終了する（ステップS154）。

図8は、携帯電話機100内において、メモ리카ード110に保持された暗号化コンテンツデータから、コンテンツデータを復号化し、音楽として外部に出力するための再生処理を説明するフローチャートである。

図8を参照して、携帯電話機100のタッチキー部1108等からのユーザ1の指示により、再生リクエストがメモ리카ード110に対して出力される（ステップS200）。

メモ리카ード110においては、この再生リクエストに応じて、コントローラ1420は、レジスタ1500に保持されるライセンス情報データLicenseに基づいて、再生可能なデータに対するリクエストであるかを判断し（ステップS202）、再生可能と判断した場合は、KPmedia(1)保持部1401から、公開暗号化鍵KPmedia(1)を携帯電話機100に対して送信する（ステップS204）。一方、再生不可能と判断した場合は、処理を終了する（ステップS230）。

再生可能と判断され、メモ리카ード110から公開暗号化鍵KPmedia(1)が送信された場合、携帯電話機100では、メモ리카ード110からの公開暗号化鍵KPmedia(1)を受信すると（ステップS206）、Ks発生部1502においてセッションキーKsを生成し、暗号化処理部1504が、公開暗号化鍵KPmedia(1)により、セッションキーKsを暗号化して暗号化セッションキー[Ks]KPmedia(1)を生成し、データバスBS2を介して、メモ리카ード110に対して送信する（ステップS208）。

メモ리카ード110は、データバスBS2を介して、携帯電話機100により生成され、かつ暗号化されたセッションキーKsを受け取り、秘密復号鍵Kmedia(1)により復号し、セッションキーKsを抽出する(ステップS210)。

- 5 続いて、メモ리카ード110は、メモリ1412から、暗号化されているデータ[Kc, License]Kcard(1)を読み出し、復号処理部1416が復号処理を行なう(ステップS212)。

- 10 秘密復号鍵Kcard(1)により、メモリ1412から読み出されたデータを復号可能な場合(ステップS214)、ライセンスキーKcが抽出される(ステップS216)。一方、再生不可能の場合、処理は終了する(ステップS232)。

メモリ1412から読み出されたデータを再生可能な場合(ステップS214)は、レジスタ1500内のライセンス情報データLicenseのうち、再生回数に関するデータが変更される(ステップS218)。

- 15 続いて、抽出したセッションキーKsにより、ライセンスキーKcを暗号化し(ステップS220)、暗号化されたライセンスキー[Kc]KsをデータバスBS2に与える(ステップS222)。

- 20 携帯電話機100の復号処理部1506は、セッションキーKsにより復号化処理を行なうことにより、ライセンスキーKcを取得する(ステップS224)。

続いて、メモ리카ード110は、暗号化コンテンツデータ[Dc]Kcをメモリ1412から読み出し、データバスBS2に与える(ステップS226)。

- 25 携帯電話機100の音楽再生部1508は、暗号化コンテンツデータ[Dc]Kcを、抽出されたライセンスキーKcにより復号処理して平文の音楽データを生成し(ステップS228)、音楽信号を再生して混合部1510に与える(ステップS230)。デジタルアナログ変換部1512は、混合部1510からのデータを受け取って変換し、外部に再生された音楽を出力し、処理が終了する(ステップS232)。

このような構成とすることで、メモ리카ード自身が、セッションキーKsを送

る側（携帯電話機１００）に、公開暗号化鍵ＫＰｍｅｄｉａ（１）を送信した上で、再生動作を行なうことが可能となる。

図９および図１０は、２つのメモ리카ード間において、音楽データおよびキーデータ等の移動または複製を行なう処理を説明するための第１および第２のフローチャートである。

まず、携帯電話機１０２が送信側であり、携帯電話機１００が受信側であるものとする。また、携帯電話機１０２にも、メモ리카ード１１０と同様の構成を有するメモ리카ード１１２が装着されているものとする。

携帯電話機１０２は、まず、自身の側のメモ리카ード１１２および携帯電話機  
１００に対して、移動リクエストまたは複製リクエストを出力する（ステップＳ  
３００）。

メモ리카ード１１２は、これに応じて、メモリ１４１２内の暗号化コンテンツ  
データ〔Ｄｃ〕Ｋｃを読み出して、メモ리카ード１１０に対して出力し（ステッ  
プＳ３０２）、一方、携帯電話機１００は、携帯電話機１０２からリクエストを  
受信して（ステップＳ３０１）、メモ리카ード１１０では、暗号化コンテンツデ  
ータ〔Ｄｃ〕Ｋｃをメモリ１４１２に格納する（ステップＳ３０４）。

続いて、携帯電話機１０２および１００においては、ステップＳ３００におい  
て与えられたリクエストが、「移動リクエスト」であるか「複製リクエスト」で  
あるかが判断され（ステップＳ３０６、ステップＳ３０６′）、「移動リクエス  
ト」である場合、メモ리카ード１１２は、公開暗号化鍵ＫＰｍｅｄｉａ（２）を  
携帯電話機１０２に対して送信し（ステップＳ３０８）、携帯電話機１０２は、  
公開暗号化鍵ＫＰｍｅｄｉａ（２）を受信する（ステップＳ３１２）。一方、メ  
モ리카ード１１０は、「移動リクエスト」である場合、公開暗号化鍵ＫＰｍｅ  
ｄｉａ（１）を携帯電話機１００に出力し（ステップＳ３０８′）、携帯電話機  
１００は、公開暗号化鍵ＫＰｍｅｄｉａ（１）を携帯電話機１０２に対して送信す  
る（ステップＳ３１０）。

携帯電話機１０２が、公開暗号化鍵ＫＰｍｅｄｉａ（１）および公開暗号化鍵  
ＫＰｍｅｄｉａ（２）を受信すると（ステップＳ３１２、ステップＳ３１２  
′）、携帯電話機１０２においては、セッションキー発生回路１５０２は、セッ

セッションキー $K_s$ を生成し（ステップS303）、公開暗号化鍵 $KPmedia$ （1）および公開暗号化鍵 $KPmedia$ （2）を用いて、暗号化処理部1504がセッションキー $K_s$ を暗号化する（ステップS314）。

5 携帯電話機102は、データバスBS2を介して、メモ리카ード112に対しては暗号化セッションキー $[K_s]$   $KPmedia$ （2）を伝達し、メモ리카ード112においては、秘密復号鍵 $Kmedia$ （2）によりセッションキー $K_s$ を復号抽出する（ステップS328）。

さらに、携帯電話機102は、暗号化セッションキー $[K_s]$   $KPmedia$ （1）を携帯電話機100に対して送信する（ステップS316）。携帯電話機100は、暗号化セッションキー $[K_s]$   $KPmedia$ （1）を受信すると（ステップS318）、メモ리카ード110に伝達し、メモ리카ード110は、復号処理部1404が復号して、セッションキー $K_s$ を受信する（ステップS320）。

メモ리카ード110においては、セッションキー $K_s$ によりメモ리카ード110の公開暗号化鍵 $KPcard$ （1）を暗号化して（ステップS322）、携帯電話機100から携帯電話機102に対して暗号化されたデータ $[KPcard$ （1）] $K_s$ を送信する（ステップS324）。携帯電話機102は、データ $[KPcard$ （1）] $K_s$ を受信し（ステップS326）、かつ、メモ리카ード112によるセッションキー $K_s$ の受信が完了すると（ステップS328）、メモ리카ード112においては、メモ리카ード110から送信された暗号化データ $[KPcard$ （1）] $K_s$ をセッションキー $K_s$ により復号化して、メモ리카ード110の公開暗号化鍵 $KPcard$ （1）を復号抽出する（ステップS330）。

25 続いて、メモ리카ード112においては、メモリ1412からメモ리카ード112の公開暗号化鍵 $KPcard$ （2）により暗号化されているライセンスキー $Kc$ 、ライセンス情報データ $License$ が読み出される（ステップS332）。

続いて、メモ리카ード112の復号処理部1416が、秘密復号鍵 $Kcard$ （2）により、ライセンスキー $Kc$ 、ライセンス情報データ $License$ を復

号処理する（ステップS 3 3 4）。

メモ리카ード1 1 2のコントローラ1 4 2 0は、このようにして復号されたライセンス情報データL i c e n s eの値を、レジスタ1 5 0 0内のデータ値と置換する（ステップS 3 3 6）。

- 5      さらに、メモ리카ード1 1 2の暗号化処理部1 4 1 4は、復号処理部1 4 1 0において抽出されたメモ리카ード1 1 0における公開暗号化鍵K P c a r d (1)により、ライセンスキーK c、ライセンス情報データL i c e n s eとを暗号化する（ステップS 3 3 8）。

- 10     メモ리카ード1 1 2の暗号化処理部1 4 1 4により暗号化されたデータは、切換スイッチ1 4 0 8（接点P cが閉じている）を介して、さらに、暗号化処理部1 4 0 6に与えられ、暗号化処理部1 4 0 6は、データ[K c, L i c e n s e] K c a r d (1)をセッションキーK sにより暗号化してデータ[[K c, L i c e n s e] K c a r d (1)] K sを生成する（ステップS 3 4 0）。

- 15     続いて、メモ리카ード1 1 2は、携帯電話機1 0 2に対してデータ[[K c, L i c e n s e] K c a r d (1)] K sを出力し（ステップS 3 4 2）、携帯電話機1 0 2はデータ[[K c, L i c e n s e] K c a r d (1)] K sを携帯電話機1 0 0に対して送信する（ステップS 3 4 4）。

- 20     携帯電話機1 0 0が受信したデータ[[K c, L i c e n s e] K c a r d (1)] K sは（ステップS 3 4 6）、メモ리카ード1 1 0に対して伝達され、メモ리카ード1 1 0の復号処理部1 4 1 0は、暗号化されたデータ[[K c, L i c e n s e] K c a r d (1)] K sを復号して、データ[K c, L i c e n s e] K c a r d (1)を受理する（ステップS 3 4 8）。

- 25     メモ리카ード1 1 0においては、復号処理部1 4 1 0により、セッションキーK sに基づいて復号化処理されたデータをメモリ1 4 1 2に記録する（ステップS 3 5 0）。さらに、メモ리카ード1 1 0においては、復号処理部1 4 1 6が、秘密復号鍵K c a r d (1)に基づいて、データ[K c, L i c e n s e] K c a r d (1)を復号し、復号されたライセンス情報データL i c e n s eをレジスタ1 5 0 0に格納する（ステップS 3 5 2）。

復号されたライセンス情報データL i c e n s eのレジスタ1 5 0 0への格納

が終了すると、メモリカード110は携帯電話機100に移動受理を通知し、携帯電話機100は、携帯電話機102に対して移動受理を送信する（ステップS354）。

5 携帯電話機102は、携帯電話機100からの移動受理を受信すると、メモリカード112に対してこれを転送し、メモリカード112は、これに応じて、レジスタ1500に格納されたライセンス情報データLicenseを消去する（ステップ358）。

10 一方、携帯電話機102では、移動受理が受信されたことに応じて、ディスプレイ1110上に、ユーザ2に対して、メモリカード112のメモリ1412内に格納されている移動データに対応する記憶データの消去を行なうかを問うメッセージを表示する。これに応じて、ユーザ2は、タッチキー1108からこのメッセージに対する回答を入力する（ステップS360）。

15 レジスタ1500内のデータの消去が完了し（ステップS358）、かつ、上記メッセージに対する回答の入力が行なわれると（ステップS360）、メモリカード112内のコントローラ1420は、メモリ1412内のデータの消去を行なうかの判断を行なう（ステップS362）。

メモリ1412内の該当データの消去が指示されている場合（ステップS362）、コントローラ1420により制御されて、メモリ1412内の暗号化コンテンツデータ[Dc]Kcおよびデータ[Kc, License]Kcard  
20 (2)が消去され（ステップS364）、処理が終了する（ステップS374）。

25 一方、メモリ1412内の該当データの消去が指示されていない場合（ステップS362）、処理は終了する（ステップS374）。この場合、メモリ1412内には、暗号化コンテンツデータ[Dc]Kcおよびデータ[Kc, License]Kcard(2)が残っていることになるが、レジスタ1500内にライセンス情報データLicenseが存在しないため、ユーザ2は、再度、音楽サーバ30から再生情報を配信してもらわない限り、音楽データの再生を行なうことはできない。すなわち、メモリカード112は「状態SB」となる。メモリカード110においては、暗号化コンテンツデータ以外にも、ライセンスキーK

c、ライセンス情報データが移動されているので、メモリカード110は「状態SA」となっている。

一方、ステップS306において、「複製リクエスト」が与えられていると判断された場合は、携帯電話機100から携帯電話機102に対して複製受取が送信される（ステップS370）。携帯電話機102において、複製受取を受信すると（ステップS372）、処理が終了する（ステップS374）。

このような構成とすることで、メモリカード自身が、セッションキーKsを送る側（携帯電話機100）に、公開暗号化鍵K<sub>Pmedia</sub>（1）およびK<sub>Pmedia</sub>（2）を送信した上で、移動動作を行なうこと、および複製動作を行なうことが可能となる。

#### [実施の形態2]

実施の形態2のデータ配信システムにおいては、実施の形態1のデータ配信システムの構成と異なって、配信サーバ、携帯電話機およびメモリカードの各々が、独自のセッションキーを生成する構成となっていることを1つの特徴とする。すなわち、配信サーバまたは携帯電話機の発生するセッションキーをセッションキーKsとし、一方のメモリカード120の発生するセッションキーをセッションキーKs1とし、メモリカード120と同様の構成を有する他方のメモリカード122の発生するセッションキーをセッションキーKs2とする。

すなわち、実施の形態2のデータ配信システムにおいては、システムを構成する機器の各々が、自身でセッションキーを生成し、データを受け取るとき、言い換えるとデータの送信先になっている場合には、相手方（送信元）に対して、まず、セッションキーを配送する。送信元は、この送信先から配送されたセッションキーでデータを暗号化し、この暗号化データを送信する。送信先では、自身で生成したセッションキーにより、受け取ったデータを復号化するという構成を1つの特徴とするものである。

また、上記のような動作を実現するために、再生動作において、携帯電話機側がメモリカードの生成するセッションキーを受け取るための公開暗号化鍵をK<sub>Pp</sub>とし、この公開暗号化鍵K<sub>Pp</sub>で暗号化されたデータを復号化できる秘密復号鍵を鍵K<sub>p</sub>とする。

図11は、実施の形態2のメモリカード120に対応した配信サーバ11の構成を示す概略ブロック図である。図3に示した配信サーバ10の構成と異なる点は、データ処理部310における暗号化処理部322は、Ks発生部314からのセッションキーKsに基づいてではなく、携帯電話機に装着されたメモリカードからセッションキーKs1、Ks2により暗号化されて送信され、復号処理部318により復号抽出されたセッションキー、たとえば、セッションキーKs1に基づいて、暗号化処理部320の出力をさらに暗号化して、データバスBS1を介して通信装置350に与える点である。

配信サーバ11のその他の点は、図3に示した実施の形態1の配信サーバ10の構成と同様であるので、同一部分には同一符号を付してその説明は繰り返さない。

図12は、実施の形態2における携帯電話機101の構成を説明するための概略ブロック図である。

図4に示した携帯電話機100の構成と異なる点は、まず、メモリカード120が装着されていること以外に、携帯電話機101は、公開暗号化鍵Kpを保持して、再生動作時に公開暗号化鍵KpをデータバスBS2に出力するKp保持部1524を備える構成となっていることである。

さらに、携帯電話機101は、秘密復号鍵Kpを保持するKp保持部1520と、このKp保持部1520から与えられる秘密復号鍵Kpに基づいて、データバスBS2を介してメモリカード120から与えられる公開暗号化鍵Kpで暗号化されたセッションキーKs1を復号し抽出する復号処理部1522とをさらに備える構成となっている。しかも、暗号化処理部1504は、この復号処理部1522から与えられるセッションキーKs1により、Ks発生部1502からの自身のセッションキーKsを暗号化してデータバスBS2に出力する。

携帯電話機101のその他の点は、図4に示した実施の形態1の携帯電話機100の構成と同様であるので、同一部分には同一符号を付してその説明は繰り返さない。

図13は、本発明の実施の形態2のメモリカード120の構成を説明するための概略ブロック図であり、実施の形態1の図5と対比される図である。



メモ리카ード120の構成が、メモ리카ード110の構成と異なる点は、まず、メモ리카ード120は、このカード独自のセッションキーKs1を発生するセッションキーKs1発生部1432を備えることである。

さらに、メモ리카ード120は、セッションキー発生回路1432で生成されたセッションキーKs1を、暗号化してデータベースBS3に与えるための暗号化処理部1430を備える。

これに応じて、メモ리카ード120は、さらに、再生モードにおいて、形態電話機101の公開暗号化鍵Kppを受けて保持するKpp受理部1407と、移動モードにおいて、相手方（移動先）の公開暗号化鍵Kpmedia(n)を受けて保持するKpmedia受理部1403と、このKpmedia受理部1403の出力とKpp受理部1407の出力とを受けて、動作モードに応じていずれか一方を出力する切換えスイッチ1436を備える。切換えスイッチ1436は、接点PiおよびPhとを有し、接点PiはKpp受理部1407と、接点PhはKpmedia受理部1403とそれぞれ結合する。暗号化処理部1430は、切換えスイッチ1436から与えられる公開暗号化鍵Kpmedia(n)または公開暗号化鍵Kppのいずれかにより、Ks1発生部1432からのセッションキーKs1を暗号化して、データベースBS3に与える。

すなわち、切換えスイッチ1436は、配信動作のとき、および移動動作において移動先となっているときは、未使用状態であり、再生動作の時は、接点Piの側に閉じており、移動動作において移動元となっているときは、接点Phの側に閉じている。

メモ리카ード120は、さらに、接点Pe、PfおよびPgを有し、復号処理部1404から与えられる音楽サーバからのセッションキーKsと、Ks1発生部1432の出力と、データベースBS4から与えられる携帯電話機101からのセッションキーKsとを受けて、動作モードに応じていずれか1つを選択的に出力する切換えスイッチ1435を備える。接点Peには復号処理部1404からの出力が、接点PfにはKs1発生部1432の出力が、接点PgにはデータベースBS4がそれぞれ結合している。したがって、暗号化処理部1406と復号処理部1410は、この切換えスイッチ1435から与えられるキーに基づいて、

それぞれ、暗号化処理および復号処理を行なう。

すなわち、切換えスイッチ1435は、配信動作の場合に音楽サーバ31からのセッションキーKs1の抽出を行なうときは、接点Peの側に閉じており、配信動作の場合に音楽サーバ31からの暗号化されたライセンスキーKc、ライセンス情報データについてセッションキーKs1による復号を行なうときは、接点Pfの側に閉じている。切換えスイッチ1435は、再生動作において復号処理を行なうときは、接点Pfの側に閉じており、再生動作において暗号化処理を行なうときは、接点Pgの側に閉じている。切換えスイッチ1435は、移動動作において移動元となっている場合に復号処理を行なうときは、接点Pfの側に閉じており、移動動作において移動元となっている場合に暗号化処理を行なうときは、接点Pgの側に閉じている。切換えスイッチ1435は、移動動作において移動先となっている場合に移動元のセッションキーを受け取るときは、接点Peの側に閉じており、移動動作において移動先となっている場合にライセンスキーKcおよびライセンス情報データLicenseを受け取るときは、接点Pfの側に閉じている。

メモリカード120は、さらに、接点Pa、Pb、PcおよびPdを有し、Ks1発生部1432から与えられる自身のセッションキーKs1と、KPcard保持部1405の出力と、データバスBS5から与えられるライセンスキーKcと、暗号化処理部1414から与えられ、相手方の公開暗号化鍵KPcard(n)により暗号化されたライセンスキーKcおよびライセンス情報データLicenseを受けて、動作モードに応じていずれか1つを選択的に出力する切換えスイッチ1409を、切換えスイッチ1408の替わりに備える。

接点PaにはKs1発生部1432からの出力が、接点PbにはKPcard(1)保持部1405の出力が、接点PcにはデータバスBS5が、接点Pdには暗号化処理部1414の出力が、それぞれ結合している。したがって、暗号化処理部1406は、この切換えスイッチ1409から与えられるデータに対して、それぞれ、暗号化処理を行なう。

すなわち、切換えスイッチ1409は、配信モードにおいて、配信先となっている場合に音楽サーバ31に自身の公開暗号化鍵KPcard(1)や自身のセ

セッションキーK s 1を送信するときは、順次、接点P bの側および接点P aの側に閉じる。切換えスイッチ1 4 0 9は、再生モードのときは、接点P cの側に閉じており、移動モードにおいて移動元となっているときは、接点P dの側に閉じている。切換えスイッチ1 4 0 9は、移動モードにおいて移動先となっている場合にも移動元に自身の公開暗号化鍵K P c a r d (1)や自身のセッションキーK s 1を送信するときは、順次、接点P bの側および接点P aの側に閉じる。

図1 4および図1 5は、図1 3で説明したメモリカード1 2 0を用いた配信モードを説明するための第1および第2のフローチャートである。

図1 4および図1 5においても、ユーザ1が、メモリカード1 2 0を用いることで、音楽サーバ3 1から音楽データの配信を受ける配信モードの動作を説明している。

まず、ユーザ1の携帯電話機1 0 1から、ユーザによりタッチキー1 1 0 8のキーボタンの操作等によって、配信リクエストがなされる（ステップS 1 0 0）。

メモリカード1 2 0においては、この配信リクエストに応じて、K P m e d i a (1)保持部1 4 0 1から、公開暗号化鍵K P m e d i a (1)を音楽サーバ3 1に対して送信する（ステップS 1 0 2）。さらに、メモリカード1 2 0においては、K s 1発生部1 4 3 2によりセッションキーK s 1が生成される（ステップS 1 0 9）。

音楽サーバ3 1では、メモリカード1 2 0から転送された配信リクエストならびに公開暗号化鍵K P m e d i a (1)を受信すると（ステップS 1 0 4）、受信した公開暗号化鍵K P m e d i a (1)に基づいて、認証サーバ1 2に対して照会を行ない、正規のメモリカードを用いたアクセスの場合は次の処理に移行し（ステップS 1 0 6）、正規のメモリカードでない場合には、処理を終了する（ステップS 1 5 4）。

照会の結果、正規のメモリカードであることが確認されると、音楽サーバ3 1では、セッションキー発生部3 1 4が、セッションキーK sを生成する。さらに、音楽サーバ3 1内の暗号化処理部3 1 6が、受信した公開暗号化鍵K P m e d i a (1)により、このセッションキーK sを暗号化して暗号化セッションキ

ー [Ks] Kmedia (1) を生成する (ステップS108)。

続いて、音楽サーバ31は、暗号化セッションキー [Ks] Kmedia (1) をデータベースBS1に与える。通信装置350は、暗号化処理部316からの暗号化セッションキー [Ks] Kmedia (1) を、通信網を通じて、携帯電話機101のメモリカード120に対して送信する (ステップS110)。

携帯電話機101が、暗号化セッションキー [Ks] Kmedia (1) を受信すると (ステップS112)、メモリカード120においては、メモリインタフェース1200を介して、データベースBS3に与えられた受信データを、復号処理部1404が、秘密復号鍵Kmedia (1) で復号処理することにより、セッションキーKsを復号し抽出する (ステップS114)。

続いて、配信モードにおいては、切換えスイッチ1409は、接点PaまたはPbが順次閉じる状態が選択されるので、暗号化処理部1406は、接点Paを介してセッションキー発生部1432から与えられるセッションキーKs1と接点Pbを介してKPcard (1) 保持部1405から与えられる公開暗号化鍵KPcard (1) (メモリカード120に対する公開暗号化鍵) とを、セッションキーKsにより暗号化し (ステップS116)、データ [KPcard (1)、Ks1] Ksを生成する (ステップS118)。

携帯電話機101は、暗号化処理部1406により暗号化されたデータ [KPcard (1)、Ks1] Ksを音楽サーバ31に対して送信する (ステップS120)。

音楽サーバ31では、通信装置350によりデータ [KPcard (1)、Ks1] Ksが受信され (ステップS122)、データベースBS1に与えられたデータ [KPcard (1)、Ks1] Ksを復号処理部318が、セッションキーKsにより復号処理して、公開暗号化鍵KPcard (1) およびセッションキーKs1を復号抽出する (ステップS124)。

続いて、配信制御部312は、配信情報データベース304等に保持されているデータを元に、ライセンスIDデータ等を含むライセンス情報データLicenseを生成する (ステップS126)。

さらに、音楽サーバ31は、暗号化コンテンツデータ [Dc] Kcを配信情報

データベース304より取得して、通信装置350を介して、メモリカード120に送信する（ステップS128）。

携帯電話機101が暗号化コンテンツデータ[Dc]Kcを受信すると（ステップS130）、メモリカード120においては、受信した暗号化コンテンツデータ[Dc]Kcをそのままメモリ1412に格納する（ステップS132）。

一方、音楽サーバ31は、ライセンスキーKcを配信情報データベース304より取得し（ステップS134）、暗号化処理部320は、配信制御部312からのライセンスキーKcとライセンス情報データLicenseとを、復号処理部318より与えられた公開暗号化鍵KCard(1)により暗号化処理する（ステップS136）。

暗号化処理部322は、暗号化処理部320により暗号化されたデータ[Kc, License]KCard(1)を受取って、さらに、メモリカード120からのセッションキーKs1により暗号化したデータをデータバスBS1に与える。通信装置350は、暗号化処理部322により暗号化されたデータ[[Kc, License]KCard(1)]Ks1をメモリカード120に対して送信する。

携帯電話機101がデータ[[Kc, License]KCard(1)]Ks1を受信すると（ステップS142）、メモリカード120においては、復号処理部1410が接点Pfを介してKs1発生部1432から与えられるセッションキーKs1により復号処理を行ない、データ[Kc, License]KCard(1)を抽出し、メモリ1412に格納する（ステップS146）。

さらに、メモリカード120においては、コントローラ1420により制御されて、復号処理部1416が、メモリ1412に格納されたデータ[Kc, License]KCard(1)を復号し、復号されたライセンス情報データLicenseを、レジスタ1500に格納する（ステップ148）。

以上のような動作により、メモリカード120自身が、暗号化コンテンツデータを送る側（音楽サーバ31）に、公開暗号化鍵KMedia(1)およびセッションキーKs1を送信した上で、配信を受けることができ、メモリカード120は、音楽情報を再生可能な状態となる。

さらに、メモリカード120から音楽サーバ31へは、配信受理が通知され、音楽サーバ31で配信受理を受信すると（ステップS150）、課金データベース302にユーザ1の課金データが格納され（ステップS152）、処理が終了する（ステップS154）。

- 5      図16および図17は、携帯電話機101内において、メモリカード120に保持された暗号化コンテンツデータから、音楽データであるコンテンツデータを復号化し、音楽として外部に出力するための再生モードを説明する第1および2のフローチャートである。

- 10      図16および図17を参照して、携帯電話機のタッチキー1108等からのユーザ1の指示により、再生リクエストがメモリカード120に対して出力される（ステップS200）。

- 15      メモリカード120においては、この再生リクエストに応じて、コントローラ1420は、レジスタ1500に保持されるライセンス情報データLicenseに基づいて、復号可能なデータに対するリクエストであるかを判断し（ステップS202）、再生可能と判断した場合は、再生可能通知を携帯電話機101に対して送信する（ステップS240）。一方、再生不可能と判断した場合は、処理を終了する（ステップS280）。

- 20      再生可能と判断され、メモリカード120から再生可能通知が送信された場合、携帯電話機101では、公開暗号化鍵K<sub>P</sub>をメモリカード120に送信し（ステップS242）、K<sub>s</sub>発生部1502においてセッションキーK<sub>s</sub>を生成する（ステップS244）。

- 25      一方、メモリカード120も、セッションキーK<sub>s</sub>1を生成する（ステップS240）。メモリカード120は、さらに、データバスBS2を介して携帯電話機101から受けとった公開暗号化鍵K<sub>P</sub>によりセッションキーK<sub>s</sub>1を暗号化し（ステップS248）、生成された暗号化セッションキー[K<sub>s</sub>1]K<sub>P</sub>を携帯電話機101に対して送信する（ステップS250）。

携帯電話機101では、メモリカード120からの暗号化セッションキー[K<sub>s</sub>1]K<sub>P</sub>を受信すると、復号処理部1522が、秘密復号鍵K<sub>P</sub>により復号化してメモリカード120で生成したセッションキーK<sub>s</sub>1を抽出する（ステップ

S 2 5 2)。続いて、携帯電話機 1 0 1 の暗号化処理部 1 5 0 4 は、携帯電話機 1 0 1 で生成したセッションキー  $K_s$  をセッションキー  $K_{s1}$  により暗号化して、暗号化セッションキー  $[K_s] K_{s1}$  を生成し (ステップ S 2 5 4)、この暗号化セッションキー  $[K_s] K_{s1}$  をメモリカード 1 2 0 に対して送信する (ステップ S 2 5 6)。

メモリカード 1 2 0 は、データバス B S 2 を介して、携帯電話機 1 0 1 により生成された暗号化セッションキー  $[K_s] K_{s1}$  を受け取り、セッションキー  $K_{s1}$  により復号し、携帯電話機 1 0 1 で生成したセッションキー  $K_s$  を抽出する (ステップ S 2 5 8)。

10 続いて、メモリカード 1 2 0 は、メモリ 1 4 1 2 から、暗号化されているデータ  $[K_c, License] K_{card}(1)$  を読み出し、復号処理部 1 4 1 6 が復号処理を行なう (ステップ S 2 6 0)。

15 秘密復号鍵  $K_{card}(1)$  により、メモリ 1 4 1 2 から読み出されたデータを復号可能な場合 (ステップ S 2 6 2)、ライセンスキー  $K_c$  が抽出される (ステップ S 2 6 4)。一方、復号不可能の場合、処理は終了する (ステップ S 2 8 0)。

メモリ 1 4 1 2 から読み出されたデータを復号可能な場合は、さらに、レジスタ 1 5 0 0 内のライセンス情報データ  $License$  のうち、再生回数に関するデータが変更される (ステップ S 2 6 6)。

20 続いて、メモリカード 1 2 0 においては、暗号化処理部 1 4 0 6 が、抽出したセッションキー  $K_s$  により、ライセンスキー  $K_c$  を暗号化し (ステップ S 2 6 8)、暗号化ライセンスキー  $[K_c] K_s$  をデータバス B S 2 に与える (ステップ S 2 7 0)。

25 携帯電話機 1 0 1 の復号処理部 1 5 0 6 は、セッションキー  $K_s$  により復号化処理を行なうことにより、ライセンスキー  $K_c$  を取得する (ステップ S 2 7 2)。

続いて、メモリカード 1 2 0 は、暗号化コンテンツデータ  $[D_c] K_c$  をメモリ 1 4 1 2 から読み出し、データバス B S 2 に与える (ステップ S 2 7 4)。

携帯電話機 1 0 1 の音楽再生部 1 5 0 8 は、暗号化コンテンツデータ  $[D_c]$

Kcを、抽出されたライセンスキーKcにより復号処理して平文のコンテンツデータを生成し（ステップS276）、音楽信号を再生して混合部1510に与える（ステップS276）。デジタルアナログ変換部1512は、混合部1510からの音楽信号を受け取って変換し、外部に再生された音楽を出力し、処理が終了する（ステップS232）。

このような構成とすることで、メモ리카ード自身および携帯電話自身が、それぞれセッションキーKs1またはKsを生成し、これにより暗号化されたデータの授受を行なった上で、再生動作を行なうことが可能となる。

図18および図19は、2つのメモ리카ード間において、コンテンツデータおよびキーデータ等の移動モードまたは複製モードを行なう処理を説明するための第1および第2のフローチャートである。

まず、携帯電話機101と同様の構成を有する携帯電話機103が送信側であり、携帯電話機101が受信側であるものとする。また、携帯電話機103にも、メモ리카ード120と同様の構成を有するメモ리카ード122が装着されているものとする。

携帯電話機103は、まず、自身の側のメモ리카ード122および携帯電話機101に対して、移動リクエストまたは複製リクエストを出力する（ステップS300）。

メモ리카ード122は、これに応じて、メモリ1412内の暗号化コンテンツデータ[Dc]Kcを読み出して、メモ리카ード120に対して出力し（ステップS302）、一方、携帯電話機101は、携帯電話機103からのリクエストを受信し（ステップS301）、メモ리카ード120では、暗号化コンテンツデータ[Dc]Kcをメモリ1412に格納する（ステップS304）。

続いて、携帯電話機103および101においては、ステップS300において与えられたリクエストが、「移動リクエスト」であるか「複製リクエスト」であるかが判断され（ステップS306、ステップS306'）、「移動リクエスト」である場合、メモ리카ード120は、公開暗号化鍵K<sub>Pmedia</sub>(1)を携帯電話機101に出力し（ステップS308）、携帯電話機101は、公開暗号化鍵K<sub>Pmedia</sub>(1)を携帯電話機103に対して送信する（ステップS



310)。

携帯電話機103が、公開暗号化鍵 $KPmedia(1)$ を受信し(ステップS312)、メモリカード122に転送すると(ステップS313)、メモリカード122の $Ks2$ 発生回路1432は、セッションキー $Ks2$ を生成し(ステップS314)、公開暗号化鍵 $KPmedia(1)$ を用いて、暗号化処理部1430がセッションキー $Ks2$ を暗号化する(ステップS315)。

携帯電話機103は、暗号化セッションキー $[Ks2] KPmedia(1)$ を携帯電話機101に対して送信する(ステップS316)。携帯電話機101は、暗号化セッションキー $[Ks2] KPmedia(1)$ を受信すると(ステップS318)、メモリカード120に伝達し、メモリカード120は、復号処理部1404が復号して、セッションキー $Ks2$ を受理し、さらに、セッションキー生成部1432で、メモリカード120におけるセッションキー $Ks1$ が生成される(ステップS320)。

メモリカード120においては、セッションキー $Ks2$ によりメモリカード120の公開暗号化鍵 $KPcard(1)$ およびセッションキー $Ks1$ を暗号化して(ステップS322)、携帯電話機101から携帯電話機103に対して暗号化されたデータ $[KPcard(1), Ks1] Ks2$ を送信する(ステップS324)。携帯電話機103は、データ $[KPcard(1), Ks1] Ks2$ を受信し(ステップS326)、メモリカード122に転送する。

メモリカード122においては、復号処理部1410が、メモリカード120から送信された暗号化データ $[KPcard(1), Ks1] Ks2$ をセッションキー $Ks2$ により復号化して、メモリカード120の公開暗号化鍵 $KPcard(1)$ 、セッションキー $Ks1$ を復号抽出する(ステップS330)。

続いて、メモリカード122においては、メモリ1412からメモリカード122の公開暗号化鍵 $KPcard(2)$ により暗号化されているライセンスキー $Kc$ 、ライセンス情報データ $Licence$ に対応する $[Kc, Licence] Kcard(2)$ が読み出される(ステップS332)。

続いて、メモリカード122の復号処理部1416が、秘密復号鍵 $Kcard(2)$ により、 $[Kc, Licence] Kcard(2)$ を復号処理する(ス

テップS334)。

メモリカード122のコントローラ1420は、このようにして復号されたライセンス情報データLicenseの値を、レジスタ1500内のデータ値と置換する(ステップS336)。

- 5       さらに、メモリカード122の暗号化処理部1414は、復号処理部1410において抽出されたメモリカード120における公開暗号化鍵KCard(1)により、ライセンスキーKc、ライセンス情報データLicenseとを暗号化する(ステップS338)。

- 10       メモリカード122の暗号化処理部1414により暗号化されたデータは、切換えスイッチ1409(接点Pdが閉じている)を介して、さらに、暗号化処理部1406に与えられ、メモリカード122の暗号化処理部1406は、データ[Kc, License]KCard(1)をセッションキーKs1により暗号化してデータ[[Kc, License]KCard(1)]Ks1を生成する(ステップS340)。

- 15       続いて、メモリカード122は、携帯電話機103に対してデータ[[Kc, License]KCard(1)]Ks1を出力し(ステップS342)、携帯電話機103はデータ[[Kc, License]KCard(1)]Ks1を携帯電話機101に対して送信する(ステップS344)。

- 20       携帯電話機101が受信したデータ[[Kc, License]KCard(1)]Ks1は(ステップS346)、メモリカード120に対して伝達され、メモリカード120の復号処理部1410は、暗号化されたデータ[[Kc, License]KCard(1)]Ks1を復号して、データ[Kc, License]KCard(1)を受理する(ステップS348)。

- 25       メモリカード120においては、復号処理部1410により、セッションキーKs1に基づいて復号化処理されたデータ[Kc, License]KCard(1)をメモリ1412に格納する(ステップS350)。さらに、メモリカード120においては、復号処理部1416が、秘密復号鍵KCard(1)に基づいて、データ[Kc, License]KCard(1)を復号し、復号されたライセンス情報データLicenseをレジスタ1500に格納する(ステッ

プ S 3 5 2)。

以後の移動モードにおける処理ならびに複製モードにおけるメモリカード 1 2 0 および 1 2 2 の処理は、図 9 および図 1 0 で説明した実施の形態 1 のメモリカード 1 1 0、1 1 2 等の処理と同様であるので、その説明は繰り返さない。

- 5       このような構成とすることで、移動元および移動先のメモリカード自身が、セッションキーをそれぞれ生成した上で、移動モードを行なうが可能となる。

- 10       したがって、データバス上で伝達されるデータのライセンスキー K c およびライセンス情報データ L i c e n s e を暗号化する鍵が、セッションごとに、かつ、機器ごとに変更されるので、ライセンスキー K c およびライセンス情報データ L i c e n s e の授受のセキュリティが一層向上するという効果がある。

- 15       しかも、以上のような構成を用いることで、たとえば、メモリカード 1 2 2 からメモリカード 1 2 0 へのデータの移動を、上述したようなセッションキー発生回路 1 5 0 2 を有する携帯電話端末を介さずに、メモリカードとメモリカードとを接続可能なインタフェース機器により行なうことも可能となり、ユーザの利便性が一層向上するという効果がある。

- 20       ここで、移動時には、再生回数を制限するライセンス情報データ内の設定については、メモリ 1 4 1 2 に記録されたライセンス情報データを、レジスタ 1 5 0 0 にて再生の都度修正された再生回数を記録したライセンス情報データに変更することで、ライセンス情報データを更新する。このようにして、メモリカード間をコンテンツデータが移動しても、再生回数に制限があるコンテンツデータの再生回数は、配信時に決められた再生回数の制限を越えることがないようにすることが可能である。

#### [実施の形態 3]

- 25       実施の形態 3 のデータ配信システムにおいては、ユーザは、配信キャリアである携帯電話会社から暗号化コンテンツデータの配信を受けるのではなく、たとえば、街頭などに設置されているコンテンツデータ販売機から暗号化コンテンツデータの供給を受ける構成となっていることを 1 つの特徴とする。

図 2 0 は、このような実施の形態 3 のデータ配信システムの構成を説明するための概念図である。なお、携帯電話機 1 0 0 およびメモリカード 1 1 0 の構成は

実施の形態１で説明したものと同様であるので、その説明は繰り返さない。

図２０を参照して、コンテンツデータ販売機２０００は、ユーザに対して配信作業における案内等を出力するためのディスプレイ２００２と、ユーザから指示を入力するためのキーボード２００４と、料金投入口２００６と、携帯電話機１  
５ ００とコネクタ１１２０を介してデータの授受を行なうための外部コネクタ２０１０とを備える。さらに、コンテンツデータ販売機２０００は、携帯電話網等の通信路を介して、販売記録等を管理するための管理サーバ２２００と接続している。

図２１は、実施の形態３のコンテンツデータ販売機２０００の構成を示す概略ブロック図である。コンテンツデータ販売機２０００は、上述したように、ディスプレイ２００２と、キーボード２００４と、料金投入口２００６からの投入金を受ける料金受理部２０２０と、外部コネクタ２０１０と、コネクタ２０１０とデータベースとの間に設けられるインタフェース部２０１２と、コンテンツデータ  
１５ （音楽データ）を所定の方式に従って暗号化したデータや、ライセンス情報データ等の配信情報を保持するための配信情報データベース３０４と、管理サーバ２２００との間で情報の授受をするための通信装置３６０と、配信情報データベース３０４および管理サーバ２２００からのデータをデータベースＢＳ１を介して受取り、所定の暗号化処理を行なうためのデータ処理部２１００とを備える。

データ処理部２１００中は、実施の形態１と同様に、データベースＢＳ１上のデータに応じて、データ処理部２１００の動作を制御するための配信制御部３１２と、配信制御部３１２に制御されて、セッションキーＫ<sub>s</sub>を発生するためのセッションキー発生部３１４と、セッションキー発生部３１４より生成されたセッションキーＫ<sub>s</sub>を、カード媒体に固有な公開暗号化鍵Ｋ<sub>Pmedia</sub>(*n*)により暗号化して、データベースＢＳ１に与えるための暗号化処理部３１６と、各ユーザ  
２５ の携帯電話機においてセッションキーＫ<sub>s</sub>により暗号化されたうえでコネクタ２０１０から与えられたデータをデータベースＢＳ１を介して受けて、復号処理を行なう復号処理部３１８と、復号処理部３１８により抽出された公開暗号化鍵Ｋ<sub>Pcard</sub>(*n*)を用いて、ライセンス情報データを配信制御部３１２に制御されて暗号化するための暗号化処理部３２０と、暗号化処理部３２０の出力を、さら

にセッションキー $K_s$ により暗号化して、データバス $BS1$ を介してコネクタ $2010$ に与える暗号化処理部 $322$ とを含む。

図 $22$ および図 $23$ は、図 $20$ および図 $21$ で説明したデータ配信システムにおける配信モードを説明するための第 $1$ および第 $2$ のフローチャートである。

- 5      図 $22$ および図 $23$ においては、ユーザ $1$ が、メモ리카ード $110$ を用いることで、コンテンツデータ販売機 $2000$ から音楽データの配信を受ける場合の動作を説明している。

まず、ユーザが、コンテンツデータ販売機 $2000$ のキーボード $2004$ のキーボタンの操作等によって、配信リクエストを指示する（ステップ $S400$ ）。

- 10      コンテンツデータ販売機 $2000$ は、メモ리카ード $110$ に対して公開暗号化鍵 $KPmedia(1)$ の送信依頼を出力する（ステップ $S402$ ）。

メモ리카ード $110$ においては、この公開暗号化鍵 $KPmedia(1)$ の送信依頼に応じて、 $KPmedia(1)$ 保持部 $1401$ から、公開暗号化鍵 $KPmedia(1)$ を携帯電話機 $100$ に対して出力する（ステップ $S406$ ）。

- 15      携帯電話機 $100$ がコンテンツデータ販売機 $2000$ に公開暗号化鍵 $KPmedia(1)$ を送信し（ステップ $S408$ ）、コンテンツデータ販売機 $2000$ が、メモ리카ード $110$ から転送された公開暗号化鍵 $KPmedia(1)$ を受信すると（ステップ $S410$ ）、ディスプレイ $2002$ を介してユーザに料金投入を案内し、料金徴収を行なう（ステップ $S412$ ）。続いて、コンテンツデータ販売機 $2000$ は、セッションキー発生部 $314$ が、セッションキー $K_s$ を生成する。さらに、コンテンツデータ販売機 $2000$ 内の暗号化処理部 $316$ が、受信した公開暗号化鍵 $KPmedia(1)$ により、このセッションキー $K_s$ を暗号化して暗号化セッションキー $[K_s]Kmedia(1)$ を生成する（ステップ $S414$ ）。

- 25      続いて、コンテンツデータ販売機 $2000$ は、暗号化セッションキー $[K_s]Kmedia(1)$ をデータバス $BS1$ に与え、コネクタ $2010$ から出力する（ステップ $S416$ ）。携帯電話機 $100$ は、この暗号化セッションキー $[K_s]Kmedia(1)$ を受信すると、メモ리카ード $110$ に転送する（ステップ $S418$ ）。

メモ리카ード110においては、メモリアンタフェース1200を介して、データバスBS3に与えられた暗号化セッションキー[Ks]Kmedia(1)を、復号処理部1404が、秘密復号鍵Kmedia(1)により復号処理することにより、セッションキーKsを復号し抽出する(ステップS420)。

- 5      続いて、配信モードにおいては、切換えスイッチ1408は、接点Paが閉じる状態が選択されているので、暗号化処理部1406は、接点Paを介してKPcard(1)保持部1405から与えられる公開暗号化鍵KPcard(1)を、セッションキーKsにより暗号化し(ステップS422)、データ[KPcard(1)]Ksを生成する(ステップS424)。

- 10     携帯電話機100は、暗号化処理部1406により暗号化されたデータ[KPcard(1)]Ksをコンテンツデータ販売機2000に対して送信する(ステップS426)。

- 15     コンテンツデータ販売機2000では、コネクタ2010を介してデータ[KPcard(1)]Ksが受信され(ステップS428)、データバスBS1に与えられたデータ[KPcard(1)]Ksを復号処理部318が、セッションキーKsにより復号処理して、公開暗号鍵KPcard(1)を復号抽出する(ステップS430)。

- 20     続いて、配信制御部312は、配信情報データベース304等に保持されているデータを元に、ライセンスIDデータ等を含むライセンス情報データLicenseを生成する(ステップS432)。

さらに、コンテンツデータ販売機2000は、暗号化コンテンツデータ[Dc]Kcを配信情報データベース304より取得して、コネクタ2010を介して、携帯電話機100に送信する(ステップS434)。

- 25     携帯電話機100が暗号化コンテンツデータ[Dc]Kcを受信すると(ステップS436)、メモ리카ード110においては、受信した暗号コンテンツデータ[Dc]Kcをそのままメモリ1412に格納する(ステップS438)。

一方、コンテンツデータ販売機2000は、ライセンスキーKcを配信情報データベース304より取得し(ステップS440)、暗号化処理部320は、配信制御部312からのライセンスキーKcとライセンス情報データLicense

eとを、復号処理部318より与えられた公開暗号化鍵K P c a r d (1)により暗号化処理する(ステップS442)。

5 暗号化処理部322は、暗号化処理部320により暗号化されたデータ[Kc、License]Kcard(1)を受取って、さらにセッションキーKsにより暗号化したデータをデータバスBS1に与え、暗号化処理部322により暗号化されたデータ[[Kc、License]Kcard(1)]Ksがメモ  
リカード110に対して送信される(ステップS446)。

10 携帯電話機100がデータ[[Kc、License]Kcard(1)]Ksを受信すると(ステップS448)、メモリカード110においては、復号処理部1410がセッションキーKsにより復号処理を行ない、データ[Kc、License]Kcard(1)を抽出し、メモリ1412に格納する(ステップS452)。

さらに、メモリカード110においては、コントローラ1420により制御されて、復号処理部1416が、メモリ1412に格納されたデータ[Kc、License]Kcard(1)を復号し、復号されたライセンス情報データLicenseを、レジスタ1500に格納する(ステップS458)。  
15

以上のような動作により、メモリカード自身が、セッションキーKsを送る側(コンテンツデータ販売機2000)に、公開暗号化鍵K P m e d i a (1)を送信した上で、配信を受けることができ、メモリカード110に格納された暗号化コンテンツデータを用いて音楽を再生可能な状態となる。  
20

さらに、メモリカード110からコンテンツデータ販売機2000へは、携帯電話機100を介して配信受理が通知され(ステップS460)、コンテンツデータ販売機2000で配信受理を受信すると(ステップS462)、管理サーバに販売記録が送信され(ステップS464)、処理が終了する(ステップS466)。  
25

以上のような構成により、ユーザは、より簡易に暗号化された音楽データ等の配信を受けることができる。

#### [実施の形態3の変形例]

実施の形態3のデータ配信システムにおいては、メモリカード110は、携帯

電話機 100 を介して、コンテンツデータ販売機 2000 から暗号化コンテンツデータの配信を受ける構成であった。

しかしながら、図 21 に示したコンテンツデータ販売機 2000 の構成において、コネクタ 2010 の代わりに、メモリカード 110 との間のインタフェースのためのメモリスロットを設ける構成とすれば、携帯電話機 100 を介することなく、メモリカード 110 とコンテンツデータ販売機 2000 とが直接データの授受を行なうことが可能である。

図 24 は、このような実施の形態 3 の変形例のコンテンツデータ販売機 2001 の構成を示す概念図である。図 20 に示した実施の形態 3 のコンテンツデータ販売機 2000 の構成と異なる点は、外部コネクタ 2010 の代わりに、メモリカードを挿入できるカードスロット 2030 が設けられ、このカードスロット 2030 がインタフェース部 2012 を介して、データバス BS1 とデータの授受をする構成となっている点である。

図 25 および図 26 は、実施の形態 3 の変形例のデータ配信システムにおける配信モードを説明するための第 1 および第 2 のフローチャートである。

図 22 および図 23 に示した実施の形態 3 の配信モードとは、携帯電話機 100 を介さずに、メモリカード 110 とコンテンツデータ販売機 2001 がデータの授受をする点を除いては、同様の処理であるので、同一処理には同一符号を付して、その説明は繰り返さない。

以上のような構成および動作により、一層簡易に、ユーザは暗号化された音楽データ等の配信を受けることができる。

しかも、メモリカードが独立して、暗号化コンテンツデータの配信を受け、格納できるので、コンテンツデータの再生を行なう手段の選択の幅が広がり、よりユーザの利便性が向上するという利点もある。

〔実施の形態 4〕

図 27 は、実施の形態 4 のコンテンツデータ販売機 3000 の構成を説明するための概略ブロック図である。図 21 に示したコンテンツデータ販売機 2000 の構成と異なる点は、対象となるメモリカードが実施の形態 2 のメモリカード 120 であり、かつ使用される端末が携帯電話機 101 である点、およびこれに対



5 応して、データ処理部2100における暗号化処理部322は、Ks発生部314からのセッションキーKsに基づいてではなく、携帯電話機に装着されたメモリカードからセッションキーKsにより暗号化されて送信され、復号処理部318により復号抽出されたセッションキー、たとえば、セッションキーKs1に基づいて、暗号化処理部320の出力をさらに暗号化して、データバスBS1を介してインタフェース部2012およびコネクタ2010に与える点である。

コンテンツデータ販売機3000のその他の点は、図21に示した実施の形態3のコンテンツデータ販売機2000の構成の構成と同様であるので、同一部分には同一符号を付してその説明は繰り返さない。

10 また、携帯電話機101およびメモリカード110の構成も実施の形態2で説明したものと同様であるので、その説明も繰り返さない。

図28および図29は、図27で説明したデータ配信システムにおける配信モードを説明するための第1および第2のフローチャートである。

15 図28および図29においては、ユーザ1が、メモリカード120を用いることで、コンテンツデータ販売機3000から音楽データの配信を受ける場合の動作を説明している。

まず、ユーザが、コンテンツデータ販売機3000のキーボード2004のキーボタンの操作等によって、配信リクエストを指示する（ステップS500）。コンテンツデータ販売機3000は、メモリカード110に対して公開暗号化鍵KPmedia(1)の送信依頼を出力する（ステップS502）。

20 メモリカード120においては、この公開暗号化鍵KPmedia(1)の送信依頼に応じて、KPmedia(1)保持部1401から、公開暗号化鍵KPmedia(1)をコンテンツデータ販売機3000に対して送信する（ステップS506）。さらに、メモリカード120においては、Ks1発生部1432によりセッションキーKs1が生成される（ステップS515）。

携帯電話機101がコンテンツデータ販売機3000に公開暗号化鍵KPmedia(1)を送信し（ステップS508）、コンテンツデータ販売機3000が、メモリカード120から転送された公開暗号化鍵KPmedia(1)を受信すると（ステップS510）、ディスプレイ2002を介してユーザに料金投

入を案内し、料金徴収を行なう（ステップS 5 1 2）。続いて、コンテンツデータ販売機3 0 0 0は、セッションキー発生部3 1 4が、セッションキーK sを生成する。さらに、コンテンツデータ販売機3 0 0 0内の暗号化処理部3 1 6が、  
5 受信した公開暗号化鍵K P m e d i a ( 1 )により、このセッションキーK sを暗号化して暗号化セッションキー [ K s ] K m e d i a ( 1 )を生成する（ステップS 5 1 4）。

続いて、コンテンツデータ販売機3 0 0 0は、暗号化セッションキー [ K s ] K m e d i a ( 1 )をデータベースB S 1に与え、コネクタ2 0 1 0から出力する（ステップS 4 1 6）。携帯電話機1 0 1は、この暗号化セッションキー [ K s ] K m e d i a ( 1 )を受信すると、メモ리카ード1 2 0に転送する（ステップS 5 1 8）。  
10

メモ리카ード1 2 0においては、メモリアインタフェース1 2 0 0を介して、データベースB S 3に与えられた暗号化セッションキー [ K s ] K m e d i a ( 1 )を、復号処理部1 4 0 4が、秘密復号鍵K m e d i a ( 1 )により復号処理することにより、セッションキーK sを復号し抽出する（ステップS 5 2 0）。  
15

続いて、暗号化処理部1 4 0 6は、K P c a r d ( 1 )保持部1 4 0 5から与えられる公開暗号化鍵K P c a r d ( 1 )およびK s 1発生部1 4 3 2からのセッションキーK s 1を、セッションキーK sにより暗号化し（ステップS 5 2 2）、データ [ K P c a r d ( 1 )、K s 1 ] K sを生成する（ステップS 5 2 4）。  
20

携帯電話機1 0 1は、暗号化処理部1 4 0 6により暗号化されたデータ [ K P c a r d ( 1 )、K s 1 ] K sをコンテンツデータ販売機3 0 0 0に対して送信する（ステップS 5 2 6）。

コンテンツデータ販売機3 0 0 0では、コネクタ2 0 1 0を介してデータ [ K P c a r d ( 1 )、K s 1 ] K sが受信され（ステップS 5 2 8）、データベースB S 1に与えられたデータ [ K P c a r d ( 1 )、K s 1 ] K sを復号処理部3 1 8が、セッションキーK sにより復号処理して、公開暗号化鍵K P c a r d ( 1 )およびセッションキーK s 1を復号抽出する（ステップS 5 3 0）。  
25

続いて、配信制御部3 1 2は、配信情報データベース3 0 4等に保持されてい

るデータを元に、ライセンスIDデータ等を含むライセンス情報データLicenseを生成する（ステップS532）。

さらに、コンテンツデータ販売機3000は、暗号化コンテンツデータ[Dc]Kcを配信情報データベース304より取得して、コネクタ2010を介して、携帯電話機101に送信する（ステップS534）。

携帯電話機101が暗号化コンテンツデータ[Dc]Kcを受信すると（ステップS536）、メモリカード120においては、受信した暗号化コンテンツデータ[Dc]Kcをそのままメモリ1412に格納する（ステップS538）。

一方、コンテンツデータ販売機3000は、ライセンスキーKcを配信情報データベース304より取得し（ステップS540）、暗号化処理部320は、配信制御部312からのライセンスキーKcとライセンス情報データLicenseとを、復号処理部318より与えられた公開暗号化鍵KPCard(1)により暗号化処理する（ステップS542）。

暗号化処理部322は、暗号化処理部320により暗号化されたデータ[Kc, License]Kcard(1)を受取って、さらにセッションキーKs1により暗号化したデータをデータベースBS1に与え、暗号化処理部322により暗号化されたデータ[[Kc, License]Kcard(1)]Ks1が携帯電話機101に対して出力される（ステップS546）。

携帯電話機101がデータ[[Kc, License]Kcard(1)]Ks1を受信すると（ステップS548）、メモリカード120においては、復号処理部1410がセッションキーKs1により復号処理を行ない、データ[Kc, License]Kcard(1)を抽出し、メモリ1412に格納する（ステップS552）。

以下の処理は、図22および図23に示した実施の形態3の処理と同様であるので、その説明は繰り返さない。

以上のような構成により、ユーザは、より簡易に暗号化された音楽データ等のコンテンツデータ配信を受けることができる。

しかも、データベース上で伝達されるデータの暗号化キーが、セッションごとに、かつ、機器ごとに変更されるので、データ授受のセキュリティが一層向上す

るという効果がある。

[実施の形態 4 の変形例]

実施の形態 4 のデータ配信システムにおいては、メモ리카ード 120 は、携帯電話機 101 を介して、コンテンツデータ販売機 3000 から暗号化コンテンツデータの配信を受ける構成であった。

しかしながら、図 27 に示したコンテンツデータ販売機 3000 の構成において、実施の形態 3 の変形例と同様に、コネクタ 2010 の代わりに、メモ리카ード 120 との間のインタフェースのためにメモリスロットを設ける構成とすれば、携帯電話機 101 を介することなく、メモ리카ード 120 とコンテンツデータ販売機 3000 とが直接データの授受を行なうことが可能である。

このような実施の形態 4 の変形例のコンテンツデータ販売機 3001 の構成は、データ処理部 2100 の構成を除いて、図 24 に示した実施の形態 3 の変形例の構成と同様である。

すなわち、実施の形態 4 の変形例のコンテンツデータ販売機 3001 の構成は、図 27 に示した実施の形態 4 のコンテンツデータ販売機 3000 の構成と異なり、外部コネクタ 2010 の代わりに、メモ리카ードを挿入できるカードスロット 2030 が設けられ、このカードスロット 2030 がインタフェース部 2012 を介して、データバス BS1 とデータの授受をする構成となっている。

図 30 および図 31 は、実施の形態 4 の変形例のデータ配信システムにおける配信モードを説明するための第 1 および第 2 のフローチャートである。

図 28 および図 29 に示した実施の形態 3 の配信モードとは、携帯電話機 101 を介さずに、メモ리카ード 120 とコンテンツデータ販売機 3001 がデータの授受をする点を除いては、同様の処理であるので、同一処理には同一符号を付して、その説明は繰り返さない。

以上のような構成および動作により、一層簡易に、ユーザは暗号化された音楽データ等の配信を受けることができる。

しかも、メモ리카ードが独立して、暗号化コンテンツデータの配信を受け、格納できるので、音楽の再生を行なう手段の選択の幅が広がり、よりユーザの利便性が向上するという利点もある。

## 〔実施の形態５〕

実施の形態５の配信サーバ１２、携帯電話機１０５およびメモリカード１４０は、以下に説明するように、実施の形態２の配信サーバ１１、携帯電話機１０１およびメモリカード１２０の構成とは、以下の点で異なることを特徴とする。

５       すなわち、実施の形態５の携帯電話機１０５では、たとえば、あらかじめ配信システムにおける認証機構等の管理部門にこの携帯電話機１０５を登録する際に、この携帯電話機１０５に割当てられた公開暗号鍵 $KP_p$ および証明データ $Crtf$ とを公開復号鍵（公開認証鍵） $KP_{master}$ により暗号化された形で記録保持する手段を有している。

10       同様に、実施の形態５のメモリカード１４０でも、たとえば、あらかじめ配信システムにおける認証機構等の管理部門にこのメモリカード１４０を登録する際に、このメモリカードに割当てられた公開暗号鍵 $KP_{media}$ および証明データ $Crtf$ とを公開復号鍵（公開認証鍵） $KP_{master}$ により暗号化された形で記録保持する手段を有している。

15       ここで、メモリカード１４０および実施の形態５の配信サーバ１２には、この公開復号鍵（公開認証鍵） $KP_{master}$ を記録保持する手段を有している。  
この公開復号鍵（公開認証鍵） $KP_{master}$ は、システム中でデータ出力を行なう全ての機器がセッションキーのやりとりに対して、相互にデータの授受を行なえる機器であることの証明と、セッションキーを相手方に送付する際に用い  
20       る暗号化鍵の獲得に用いるシステム共通の復号鍵である。

以下、さらに、実施の形態５の携帯電話機１０５、メモリカード１４０および配信サーバ１２の構成をより詳しく説明する。

図３２は、実施の形態５における携帯電話機１０５の構成を説明するための概略ブロック図である。

25       図１２に示した実施の形態２の携帯電話機１０１の構成と異なる点は、 $KP_p$ 保持部１５２４の替わりに、公開復号鍵（公開認証鍵） $KP_{master}$ により暗号化された、公開暗号鍵 $KP_p$ および証明データ $Crtf$ を保持するための  
〔 $KP_p$ ,  $Crtf$ 〕 $KP_{master}$ 保持部１５２５を備える構成となっていることである。

携帯電話機 105 のその他の点は、図 12 に示した実施の形態 2 の携帯電話機 101 の構成と同様であるので、同一部分には同一符号を付してその説明は繰り返さない。

図 33 は、実施の形態 5 のメモリカード 140 に対応した配信サーバ 12 の構成を示す概略ブロック図である。図 11 に示した実施の形態 2 の配信サーバ 11 の構成と異なる点は、データ処理部 310 は、公開復号鍵  $KP_{master}$  を保持する  $KP_{master}$  保持部 324 と、 $KP_{master}$  保持部 324 から出力される公開復号鍵  $KP_{master}$  に基づいて、通信網から通信装置 350 を介してデータバス  $BS1$  に与えられるデータを復号するための復号処理部 326 とをさらに備える構成となっている点である。暗号化処理部 316 は、復号処理部 326 での復号処理により抽出された公開暗号化鍵  $KP_{media}$  により、 $K_s$  発生部 314 で発生されたセッションキー  $K_s$  を暗号化し、また、配信制御部 312 は、復号処理部 326 での復号処理により抽出された証明データ  $Crtf$  により、配信を求めてきたメモリカードおよび携帯電話機が正規であるかの認証を行なう。

配信サーバ 12 のその他の点は、図 12 に示した実施の形態 2 の配信サーバ 11 の構成の構成と同様であるので、同一部分には同一符号を付してその説明は繰り返さない。

図 34 は、本発明の実施の形態 5 のメモリカード 140 の構成を説明するための概略ブロック図であり、実施の形態 2 の図 13 と対比される図である。

実施の形態 5 のメモリカード 140 の構成が、実施の形態 2 のメモリカード 120 の構成と異なる点は、まず、メモリカード 140 は、公開暗号鍵  $KP_{media}$  および証明データ  $Crtf$  とを公開復号鍵（公開認証鍵） $KP_{master}$  により暗号化された形で記録保持する  $[KP_{media}, Crtf] KP_{master}$  保持部 1442 を備える構成となっていることである。一方で、切換スイッチ 1436 は省略され、 $[KP_{media}, Crtf] KP_{master}$  保持部 1442 の出力は直接データバス  $BS3$  に与えられる。

さらに、メモリカード 140 は、公開復号鍵  $KP_{master}$  を記録保持するための  $KP_{master}$  保持部 1450 と、 $KP_{master}$  保持部 1450 か

ら出力される公開復号鍵K P m a s t e rに基づいて、データベースB S 3上のデータを復号するための復号処理部1 4 5 2とを備える。

5 復号処理部1 4 5 2での復号処理により抽出される公開暗号化鍵K P m e d i aおよび証明データC r t fのうち、公開暗号化鍵K P m e d i aは、暗号化処理部1 4 3 0に与えられ、証明データC r t fは、データベースB S 5を介して、コントローラ1 4 2 0に与えられる。

メモ리카ード1 4 0のその他の構成は、図1 3に示したメモ리카ード1 2 0の構成と同様であるので、同一部分には同一符号を付してその説明は繰り返さない。

#### 10 [配信モード]

図3 5および図3 6は、図3 4で説明したメモ리카ード1 4 0を用いた配信モードを説明するための第1および第2のフローチャートである。

15 図3 5および図3 6においても、ユーザ1が、メモ리카ード1 4 0を装着した携帯電話機1 0 5にて配信サーバ1 2からコンテンツデータの配信を受ける場合の動作を説明している。

まず、ユーザ1の携帯電話機1 0 5から、ユーザによりタッチキー1 1 0 8のキーボタンの操作等によって、配信リクエストがなされる（ステップS 1 0 0）。

20 また、メモ리카ード1 4 0において保持される公開暗号化鍵K P m e d i aは、他のメモ리카ードにおける公開暗号化鍵K P m e d i aと区別するために公開暗号化鍵K P m e d i a（1）としている。さらに、メモ리카ード1 4 0、携帯電話機1 0 5における証明データをそれぞれC r t f（1）、C r t f（p）とする。

25 メモ리카ード1 4 0においては、この配信リクエストに応じて、[K P m e d i a, C r t f] K P m a s t e r保持部1 4 4 2から、公開暗号化鍵K P m e d i a（1）および証明データC r t f（1）を暗号化したデータ[K P m e d i a（1）, C r t f（1）] K P m a s t e rを携帯電話機1 0 5に対して出力する（ステップS 1 0 2）。

携帯電話機1 0 5では、メモ리카ード1 4 0からのデータ[K P m e d i a

(1), C r t f (1)] K P m a s t e r とともに、[K P p, C r t f] K P m a s t e r 保持部 1 5 2 5 からのデータ [K P p, C r t f (p)] K P m a s t e r、配信リクエストを配信サーバ 1 2 に対して送信する (ステップ S 1 0 3)。

- 5 配信サーバ 1 2 では、メモリカード 1 4 0 から転送された配信リクエストならびにデータ [K P p, C r t f (p)] K P m a s t e r、[K P m e d i a (1), C r t f (1)] K P m a s t e r を受信すると (ステップ S 1 0 4)、公開復号鍵 K P m a s t e r により復号処理部 3 2 6 が復号処理を行い、証明データ C r t f (1)、C r t f (p)、公開暗号化鍵 K P p、公開暗号化鍵 K P m e d i a (1) の抽出を行なう (ステップ S 1 0 5)。

- 10 復号された証明データ C r t f (1) および C r t f (p) に基づいて、配信制御部 3 1 2 は、配信サーバ 1 2 に対して照会を行ない、メモリカードと携帯電話機の証明データ C r t f (1) および C r t f (p) がともに正規の証明データの場合は次の処理に移行し (ステップ S 1 0 6)、いずれかが正規の証明データでない場合には、処理を終了する (ステップ S 1 5 4)。

- 15 照会の結果、正規の証明データであることが確認されると、配信サーバ 1 2 では、セッションキー発生部 3 1 4 が、セッションキー K s を生成する。さらに、配信サーバ 1 2 内の暗号化処理部 3 1 6 が、受信した公開暗号化鍵 K P m e d i a (1) により、このセッションキー K s を暗号化して暗号化セッションキー [K s] K m e d i a (1) を生成する (ステップ S 1 0 8)。

- 20 続いて、配信サーバ 1 2 は、暗号化セッションキー [K s] K m e d i a (1) をデータベース B S 1 に与える。通信装置 3 5 0 は、暗号化処理部 3 1 6 からの暗号化セッションキー [K s] K m e d i a (1) を、通信網を通じて、携帯電話機 1 0 5 のメモリカード 1 4 0 に対して送信する (ステップ S 1 1 0)。

- 25 携帯電話機 1 0 5 が、暗号化セッションキー [K s] K m e d i a (1) を受信すると (ステップ S 1 1 2)、メモリカード 1 4 0 においては、メモリインタフェース 1 2 0 0 を介して、データベース B S 3 に与えられた受信データを、復号処理部 1 4 0 4 が、秘密復号鍵 K m e d i a (1) で復号処理することにより、セッションキー K s を復号し抽出する (ステップ S 1 1 4)。



さらに、メモリカード140においては、Ks1発生部1432によりセッションキーKs1が生成される（ステップS115）。

5 続いて、配信モードにおいては、切換スイッチ1409は、接点PaまたはPbが順次閉じる状態が選択されるので、暗号化処理部1406は、接点Paを介してセッションキー発生部1432から与えられるセッションキーKs1と接点Pbを介してKPcard(1)保持部1405から与えられる公開暗号化鍵KPcard(1)（メモリカード140に対する公開暗号化鍵）とを、セッションキーKsにより暗号化し（ステップS116）、データ[KPcard(1)、Ks1]Ksを生成する（ステップS118）。

10 携帯電話機105は、暗号化処理部1406により暗号化されたデータ[KPcard(1)、Ks1]Ksを配信サーバ12に対して送信する（ステップS120）。

配信サーバ12では、通信装置350によりデータ[KPcard(1)、Ks1]Ksが受信され（ステップS122）、データバスBS1に与えられたデータ[KPcard(1)、Ks1]Ksを復号処理部318が、セッションキーKsにより復号処理して、公開暗号化鍵KPcard(1)およびセッションキーKs1を復号抽出する（ステップS124）。

15 続いて、配信制御部312は、配信情報データベース304等に保持されているデータを元に、ライセンスIDデータ等を含むライセンス情報データLicenseを生成する（ステップS126）。

20 さらに、配信サーバ12は、暗号化コンテンツデータ[Dc]Kcを配信情報データベース304より取得して、通信装置350を介して、メモリカード140に送信する（ステップS128）。

25 携帯電話機105が暗号化コンテンツデータ[Dc]Kcを受信すると（ステップS130）、メモリカード140においては、受信した暗号化コンテンツデータ[Dc]Kcをそのままメモリ1412に格納する（ステップS132）。

一方、配信サーバ12は、ライセンスキーKcを配信情報データベース304より取得し（ステップS134）、暗号化処理部320は、配信制御部312からのライセンスキーKcとライセンス情報データLicenseとを、復号処理

部318より与えられた公開暗号化鍵K P c a r d (1)により暗号化处理する  
(ステップS136)。

5 暗号化处理部322は、暗号化处理部320により暗号化されたデータ[K  
c、L i c e n s e] K c a r d (1)を受取って、さらに、メモ리카ード14  
0からのセッションキーK s 1により暗号化したデータをデータバスB S 1に与  
える。通信装置350は、暗号化处理部322により暗号化されたデータ[[K  
c、L i c e n s e] K c a r d (1)] K s 1をメモ리카ード140に対して  
送信する。

10 携帯電話機105がデータ[[Kc、L i c e n s e] K c a r d (1)] K  
s 1を受信すると(ステップS142)、メモ리카ード140においては、復号  
処理部1410が接点P fを介してK s 1発生部1432から与えられるセッ  
ションキーK s 1により復号処理を行ない、データ[Kc、L i c e n s e] K c  
a r d (1)を抽出し、メモリ1412に格納する(ステップS146)。

15 さらに、メモ리카ード140においては、コントローラ1420により制御さ  
れて、復号処理部1416が、メモリ1412に格納されたデータ[Kc、L i  
c e n s e] K c a r d (1)を復号し、復号されたライセンス情報データL i  
c e n s eを、レジスタ1500に格納する(ステップ148)。

20 以上のような動作により、メモ리카ード140自身が、暗号化コンテンツデー  
タを送る側(配信サーバ12)に、公開暗号化鍵K P m e d i a (1)およびセ  
ッションキーK s 1を送信した上で、配信を受けることができ、メモ리카ード1  
40は、音楽を再生可能な状態となる。

25 さらに、メモ리카ード140から配信サーバ12へは、配信受理が通知され、  
配信サーバ12で配信受理を受信すると(ステップS150)、課金データベー  
ス302にユーザ1の課金データが格納され(ステップS152)、処理が終了  
する(ステップS154)。

以上のような配信モードでは、メモ리카ードおよび携帯電話機の認証がなされ  
た上でコンテンツデータの配信が行われるので、システムのセキュリティおよび  
著作権の保護がより強化される。

[再生モード]

図37および図38は、携帯電話機105内において、メモ리카ード140に保持された暗号化コンテンツデータから、音楽信号を復号化し、音楽として外部に出力するための再生処理を説明する第1および第2のフローチャートである。

図37および図38を参照して、携帯電話機105のタッチキー1108等からのユーザ1の指示により、再生リクエストが携帯電話機105に対して出力される(ステップS200)。

これに応じて携帯電話機105からは、メモ리카ード140に対して、データ[KPp, Crtf(p)] KPmasterが送信される(ステップS241)。

10     メモ리카ード140においては、データ[KPp, Crtf(p)] KPmasterを受信すると、復号処理部1452により復号処理が行われ、公開暗号化鍵KPpおよびデータCrtfの抽出が行われる(ステップS243)。

抽出された証明データCrtfに基づいて、コントローラ1420は、携帯電話機105が正規の機器であるかを判断し(ステップS245)、正規の機器と判断した場合は、処理は次のステップS246に移行し、正規の機器でないと判断した場合は、処理を終了する(ステップS280)。

15     正規の機器であると判断された場合、メモ리카ード140では、セッションキーKs1を生成する(ステップS246)。メモ리카ード140は、さらに、抽出された公開暗号化鍵KPpによりセッションキーKs1を暗号化し(ステップS248)、生成された暗号化セッションキー[Ks1] Kpを携帯電話機105に対して送信する(ステップS250)。

20     携帯電話機105では、メモ리카ード140からの暗号化セッションキー[Ks1] Kpを受信すると、復号処理部1522が、秘密復号鍵Kpにより復号化してメモ리카ード140で生成したセッションキーKs1を抽出する(ステップS252)。続いて、Ks発生部1502がセッションキーKsを生成し(ステップS253)、携帯電話機105の暗号化処理部1504は、携帯電話機105で生成したセッションキーKsをセッションキーKs1により暗号化して、暗号化セッションキー[Ks] Ks1を生成し(ステップS254)、この暗号化セッションキー[Ks] Ks1をメモ리카ード140に対して送信する(ステッ

ブ S 2 5 6)。

メモリカード 1 4 0 は、データバス B S 2 を介して、携帯電話機 1 0 5 により生成され、かつ暗号化されたセッションキー K s を受け取り、セッションキー K s 1 により復号し、携帯電話機 1 0 5 で生成したセッションキー K s を抽出する  
5 (ステップ S 2 5 8)。

続いて、メモリカード 1 4 0 において、コントローラ 1 4 2 0 は、レジスタ 1 5 0 0 に保持されるライセンス情報データ L i c e n s e に基づいて、復号可能であるかを判断し (ステップ S 2 5 9)、復号可能と判断した場合は、次の処理に移行し、復号不可能と判断した場合は、処理を終了する (ステップ S 2 8  
10 0)。

続いて、メモリカード 1 4 0 は、メモリ 1 4 1 2 から、暗号化されているデータ [K c, L i c e n s e] K c a r d (1) を読み出し、復号処理部 1 4 1 6 が復号処理を行なう (ステップ S 2 6 0)。

秘密復号鍵 K c a r d (1) により、メモリ 1 4 1 2 から読み出されたデータを復号可能な場合 (ステップ S 2 6 2)、ライセンスキー K c が抽出される (ステップ S 2 6 4)。一方、復号不可能の場合、処理は終了する (ステップ S 2 8  
15 0)。

メモリ 1 4 1 2 から読み出されたデータを復号可能な場合は、さらに、レジスタ 1 5 0 0 内のライセンス情報データ L i c e n s e のうち、再生回数に関するデータが変更される (ステップ S 2 6 6)。  
20

続いて、メモリカード 1 4 0 においては、暗号化処理部 1 4 0 6 が、抽出したセッションキー K s により、ライセンスキー K c を暗号化し (ステップ S 2 6 8)、暗号化されたライセンスキー [K c] K s をデータバス B S 2 に与える (ステップ S 2 7 0)。

携帯電話機 1 0 5 の復号処理部 1 5 0 6 は、セッションキー K s により復号化処理を行なうことにより、ライセンスキー K c を取得する (ステップ S 2 7  
25 2)。

続いて、メモリカード 1 4 0 は、暗号化コンテンツデータ [D c] K c をメモリ 1 4 1 2 から読み出し、データバス B S 2 に与える (ステップ S 2 7 4)。

携帯電話機 105 の音楽再生部 1508 は、暗号化コンテンツデータ [Dc] Kc を、抽出されたライセンスキー Kc により復号処理して平文のコンテンツデータを生成し (ステップ S276)、コンテンツデータから音楽信号を再生して混合部 1510 に与える (ステップ S276)。デジタルアナログ変換部 1512 は、混合部 1510 からのデータを受け取って変換し、外部に再生された音楽を出力し、処理が終了する (ステップ S232)。

このような構成とすることで、メモ리카ード自身および携帯電話自身が、それぞれセッションキー Ks1 または Ks を生成し、これにより暗号化コンテンツデータの授受を行なった上で、再生動作を行なうことが可能となる。

さらに、メモ리카ード 140 が携帯電話機 105 の認証を行なった上で、再生動作を行なうため、システムのセキュリティおよび著作権の保護が向上する。

[移動または複製モード]

図 39 および図 40 は、2 つのメモ리카ード間において、コンテンツデータおよびキーデータ等の移動または複製を行なう処理を説明するための第 1 および第 2 のフローチャートである。

まず、携帯電話機 105 と同様の構成を有する携帯電話機 106 が送信側であり、携帯電話機 105 が受信側であるものとする。また、携帯電話機 106 にも、メモ리카ード 140 と同様の構成を有するメモ리카ード 142 が装着されているものとする。

携帯電話機 106 は、まず、携帯電話機 105 に対して、移動リクエストまたは複製リクエストを出力する (ステップ S300)。

携帯電話機 105 がこのリクエストを受信すると (ステップ S301)、メモ리카ード 142 は、これに応じて、メモリ 1412 内の暗号化コンテンツデータ [Dc] Kc を読み出して、メモ리카ード 140 に対して出力し (ステップ S302)、メモ리카ード 140 では、暗号化コンテンツデータ [Dc] Kc をメモリ 1412 に格納する (ステップ S304)。

続いて、携帯電話機 106 および 105 においては、ステップ S300 において与えられたリクエストが、「移動リクエスト」であるか「複製リクエスト」であるかが判断され (ステップ S306、ステップ S306')、「移動リクエス

ト」である場合、メモリカード140は、この移動リクエストに応じて、[KPmedia, Crtf] KPmaster保持部1442から、公開暗号化鍵KPmedia(1)および証明データCrtf(1)を暗号化したデータ[KPmedia(1), Crtf(1)] KPmasterを携帯電話機105に対して出力する(ステップS307)。

携帯電話機105では、メモリカード140からのデータ[KPmedia(1), Crtf(1)] KPmasterを携帯電話機106に対して送信する(ステップS308)。

携帯電話機106では、メモリカード140から転送されたデータ[KPmedia(1), Crtf(1)] KPmasterを受信すると(ステップS309)、メモリカード142内の復号処理部1452が復号処理を行い、証明データCrtf(1)、公開暗号化鍵KPmedia(1)の抽出を行なう(ステップS310)。

復号された証明データCrtf(1)に基づいて、コントローラ1420は、認証を行ない、正規メモリカードからのアクセスの場合は次の処理に移行し(ステップS311)、正規メモリカードでない場合には、携帯電話機106は移動不可の通知を送信するとともに、メモリカード142は処理を終了する(ステップS374)。携帯電話機105が移動不可通知を受信すると(ステップS313)、メモリカード140も処理を終了する(ステップS374)。

一方、ステップS311での照会の結果、正規メモリカードであることが確認されると、メモリカード142のKs2発生回路1432は、セッションキーKs2を生成し(ステップS314)、公開暗号化鍵KPmedia(1)を用いて、暗号化処理部1430がセッションキーKs2を暗号化する(ステップS315)。

携帯電話機106は、暗号化セッションキー[Ks2] KPmedia(1)を携帯電話機105に対して送信する(ステップS316)。携帯電話機105は、暗号化セッションキー[Ks2] KPmedia(1)を受信すると(ステップS318)、メモリカード140に伝達し、メモリカード140は、復号処理部1404が復号して、セッションキーKs2を受信する(ステップS32

0)。さらに、メモリカード140においてセッションキーKs1が生成される(ステップS321)。

メモリカード140においては、セッションキーKs2によりメモリカード140の公開暗号化鍵KPCard(1)およびセッションキーKs1を暗号化して(ステップS322)、携帯電話機105から携帯電話機106に対して暗号化されたデータ[KPCard(1)、Ks1]Ks2を送信する(ステップS324)。携帯電話機106は、データ[KPCard(1)、Ks1]Ks2を受信し(ステップS326)、メモリカード142に転送する。

メモリカード142においては、復号処理部1410が、メモリカード140から送信された暗号化データ[KPCard(1)、Ks1]Ks2をセッションキーKs2により復号化して、メモリカード140の公開暗号化鍵KPCard(1)、セッションキーKs1を復号抽出する(ステップS330)。

続いて、メモリカード142においては、メモリ1412からメモリカード142の公開暗号化鍵KPCard(2)により暗号化されているライセンスキーKc、ライセンス情報データLicenseに対応する[Kc、License]Kcard(2)読出される(ステップS332)。

続いて、メモリカード142の復号処理部1416が、秘密復号鍵Kcard(2)により、ライセンスキーKc、ライセンス情報データLicenseを復号処理する(ステップS334)。

メモリカード142のコントローラ1420は、このようにして復号されたライセンス情報データLicenseの値を、レジスタ1500内のデータ値と置換する(ステップS336)。

さらに、メモリカード142の暗号化処理部1414は、復号処理部1410において抽出されたメモリカード140における公開暗号化鍵KPCard(1)により、ライセンスキーKc、ライセンス情報データLicenseとを暗号化する(ステップS338)。

メモリカード142の暗号化処理部1414により暗号化されたデータは、切換スイッチ1409(接点Pdが閉じている)を介して、さらに、暗号化処理部1406に与えられ、メモリカード142の暗号化処理部1406は、データ

[Kc, License] Kcard (1) をセッションキーKs1により暗号化してデータ [[Kc, License] Kcard (1)] Ks1を生成する (ステップS340)。

5 続いて、メモ리카ード142は、携帯電話機106に対してデータ [[Kc, License] Kcard (1)] Ks1を出力し (ステップS342)、携帯電話機106はデータ [[Kc, License] Kcard (1)] Ks1を携帯電話機105に対して送信する (ステップS344)。

10 携帯電話機105が受信したデータ [[Kc, License] Kcard (1)] Ks1は (ステップS346)、メモ리카ード140に対して伝達され、メモ리카ード140の復号処理部1410は、暗号化されたデータ [[Kc, License] Kcard (1)] Ks1を復号して、データ [Kc, License] Kcard (1) を受取する (ステップS348)。

15 メモ리카ード140においては、復号処理部1410により、セッションキーKs1に基づいて復号化処理されたデータ [Kc, License] Kcard (1) をメモリ1412に格納する (ステップS350)。さらに、メモ리카ード140においては、復号処理部1416が、秘密復号鍵Kcard (1) に基づいて、データ [Kc, License] Kcard (1) を復号し、復号されたライセンス情報データLicenseをレジスタ1500に格納する (ステップS352)。

20 以後の移動モードにおける処理ならびに複製モードにおけるメモ리카ード140および142の処理は、図18および図19で説明した実施の形態2のメモ리카ード120、122等の処理と同様であるので、その説明は繰り返さない。

25 このような構成とすることで、移動元および移動先のメモ리카ード自身が、セッションキーをそれぞれ生成した上で、移動動作を行なうこと、および複製動作を行なうことが可能となる。

したがって、データバス上で伝達されるデータの暗号化キーが、セッションごとに、かつ、機器ごとに変更されるので、データ授受のセキュリティが一層向上するという効果がある。

しかも、以上のような構成を用いることで、たとえば、メモ리카ード142か



らメモリカード140へのデータの移動を、上述したようなセッションキー発生回路1502を有する携帯電話端末を介さずに、メモリカードとメモリカードとを接続可能なインタフェース機器により行なうことも可能となり、ユーザの利便性が一層向上するという効果がある。

- 5       ここで、移動モード時には、再生情報内の再生回数を制限するライセンス情報データについては、メモリ1412に記録されたライセンス情報データを、レジスタ1500にて再生の都度修正された再生回数を記録したライセンス情報データに変更することでライセンス情報データを更新する。このようにして、メモリカード間をコンテンツデータが移動しても、再生回数に制限があるコンテンツデータの再生回数は、配信時に決められた再生回数の制限を越えることがないようにすることが可能である。

しかも、メモリカード142がメモリカード140の認証を行った上で、移動動作を行なうため、システムのセキュリティおよび著作権の保護が向上する。

〔実施の形態6〕

- 15       図41は、本発明の実施の形態6のコンテンツデータ販売機3010の構成を示す概略ブロック図であり、実施の形態4の図27と対比される図である。

ただし、以下の説明では、実施の形態5で説明したメモリカード140との間のインタフェースのためにメモリスロット2030を設ける構成とし、実施の形態4の変形例と同様に、携帯電話機105を介することなく、メモリカード140とコンテンツデータ販売機3010とが直接データの授受を行なう構成であるものとする。

もちろん、コネクタ2010により、携帯電話機105を介して、メモリカード140とコンテンツデータ販売機3010とがデータの授受を行なう構成とすることも可能である。

- 25       したがって、コンテンツデータ販売機3010の構成が、実施の形態4のコンテンツデータ販売機3000の構成と異なる点は、コネクタ2010の代わりに、メモリスロット2030が設けられていることと、データ処理部2100は、公開復号鍵K P m a s t e rを保持するK P m a s t e r保持部324と、K P m a s t e r保持部324から出力される公開復号鍵K P m a s t e rに基

づいて、通信網から通信装置 350 を介してデータバス B S 1 に与えられるデータを復号するための復号処理部 326 とをさらに備える構成となっている点である。暗号化処理部 316 は、復号処理部 326 での復号処理により抽出された公開暗号化鍵 K P m e d i a により、K s 発生部 314 で発生されたセッションキー K s を暗号化し、また、配信制御部 312 は、復号処理部 326 での復号処理により抽出された証明データ C r t f により、配信を求めてきたメモリカードが正規のメモリカードであるかの認証を行なう。

コンテンツデータ販売機 3010 のその他の点は、図 27 に示した実施の形態 4 のコンテンツデータ販売機 3000 の構成と同様であるので、同一部分には同一符号を付してその説明は繰り返さない。

[配信モード]

図 42 および図 43 は、図 41 で説明したコンテンツデータ販売機 3010 を用いたデータ配信システムにおける配信動作を説明するための第 1 および第 2 のフローチャートである。

図 42 および図 43 においては、ユーザ 1 が、メモリカード 140 を用いることで、コンテンツデータ販売機 3010 からコンテンツデータ（音楽データ）の配信を受ける場合の動作を説明している。

まず、ユーザが、コンテンツデータ販売機 3010 のキーボード 2004 のキーボタンの操作等によって、配信リクエストを指示する（ステップ S500）。

コンテンツデータ販売機 3010 からは、メモリカード 140 に対して、認証のためのデータ [K P m e d i a , C r t f] K P m a s t e r の送信依頼が出力される（ステップ S502）。

メモリカード 140 においては、この送信依頼に応じて、[K P m e d i a , C r t f] K P m a s t e r 保持部 1442 から、公開暗号化鍵 K P m e d i a (1) および証明データ C r t f (1) を暗号化したデータ [K P m e d i a (1) , C r t f (1)] K P m a s t e r をコンテンツデータ販売機 3010 に対して出力する（ステップ S507）。

コンテンツデータ販売機 3010 では、メモリカード 140 から転送されたデータ [K P m e d i a (1) , C r t f (1)] K P m a s t e r を受信する

と、公開復号鍵K P m a s t e rにより復号処理部3 2 6が復号処理を行い、証明データC r t f ( 1)、公開暗号化鍵K P p、公開暗号化鍵K P m e d i a ( 1)の抽出を行なう(ステップS 5 0 9)。

5 復号された証明データC r t f ( 1)に基づいて、配信制御部3 1 2は、正規メモリカードからのアクセスかどうかの判断を行なう。正規のメモリカードの場合は次の処理に移行し(ステップS 5 1 1)、正規メモリカードでない場合には、管理サーバ2 2 0 0中の管理データベースに異常終了記録を格納し(ステップS 5 6 1)、処理を終了する(ステップS 5 6 2)。

10 コンテンツデータ販売機3 0 1 0は、ステップS 5 1 1での照会の結果、正規メモリカードであることが確認されると、ディスプレイ2 0 0 2を介してユーザーに料金投入を案内し、料金徴収を行なう(ステップS 5 1 2)。

続いて、コンテンツデータ販売機3 0 1 0は、セッションキー発生部3 1 4が、セッションキーK sを生成する。さらに、コンテンツデータ販売機3 0 1 0内の暗号化処理部3 1 6が、受信した公開暗号化鍵K P m e d i a ( 1)により、このセッションキーK sを暗号化して暗号化セッションキー[K s] K m e d i a ( 1)を生成する(ステップS 5 1 4)。

続いて、コンテンツデータ販売機3 0 1 0は、暗号化セッションキー[K s] K m e d i a ( 1)をデータベースB S 1に与え、カードスロット2 0 3 0から出力する(ステップS 5 1 6)。

20 メモリカード1 4 0においては、メモリインタフェース1 2 0 0を介して、データベースB S 3に与えられた暗号化セッションキー[K s] K m e d i a ( 1)を、復号処理部1 4 0 4が、秘密復号鍵K m e d i a ( 1)により復号処理することにより、セッションキーK sを復号し抽出する(ステップS 5 2 0)。さらに、メモリカード1 4 0では、セッションキーK s 1が生成される(ステップS 5 2 1)。

25 続いて、配信モードにおいては、切換スイッチ1 4 0 8は、接点P aが閉じる状態が選択されているので、暗号化処理部1 4 0 6は、接点P aを介してK P c a r d ( 1)保持部1 4 0 5から与えられる公開暗号化鍵K P c a r d ( 1)を、セッションキーK sにより暗号化し(ステップS 5 2 2)、データ[K P c

ard (1)] Ksを生成する(ステップS524)。

コンテンツデータ販売機3010では、カードスロット2030を介してデータ[KPcard (1)] Ksが受信され(ステップS528)、データベースBS1に与えられたデータ[KPcard (1)] Ksを復号処理部318が、セッションキーKsにより復号処理して、公開暗号化鍵KPcard (1)を復号抽出する(ステップS530)。

続いて、配信制御部312は、配信情報データベース304等に保持されているデータを元に、ライセンスIDデータ等を含むライセンス情報データLicenseを生成する(ステップS532)。

さらに、コンテンツデータ販売機3010は、暗号化コンテンツデータ[Dc] Kcを配信情報データベース304より取得して、カードスロット2030を介して、メモリカード140に送信する(ステップS534)。

メモリカード140においては、受信した暗号化コンテンツデータ[Dc] Kcをそのままメモリ1412に格納する(ステップS538)。

一方、コンテンツデータ販売機3010は、ライセンスキーKcを配信情報データベース304より取得し(ステップS540)、暗号化処理部320は、配信制御部312からのライセンスキーKcとライセンス情報データLicenseとを、復号処理部318より与えられた公開暗号化鍵KPcard (1)により暗号化処理する(ステップS542)。

暗号化処理部322は、暗号化処理部320により暗号化されたデータ[Kc, License] Kcard (1)を受取って、さらにセッションキーKsにより暗号化したデータをデータベースBS1に与え、暗号化処理部322により暗号化されたデータ[[Kc, License] Kcard (1)] Ks1がメモリカード140に対して送信される(ステップS546)。

メモリカード140においては、復号処理部1410がセッションキーKs1により復号処理を行ない、データ[Kc, License] Kcard (1)を抽出し、メモリ1412に格納する(ステップS552)。

さらに、メモリカード140においては、コントローラ1420により制御されて、復号処理部1416が、メモリ1412に格納されたデータ[Kc, L

cense] Kcard (1) を復号し、復号されたライセンス情報データ License を、レジスタ 1500 に格納する (ステップ S554)。

以上のような動作により、メモリカード 140 は、コンテンツデータから音楽を再生可能な状態となる。

- 5       さらに、メモリカード 140 からコンテンツデータ販売機 3010 へは、配信受理が通知され (ステップ S558)、コンテンツデータ販売機 3010 で配信受理を受信すると、管理サーバ 2200 中の管理データベースに販売記録が送信され (ステップ S560)、処理が終了する (ステップ S562)。

- 10       以上のような構成により、ユーザは、より簡易に暗号化された音楽データ等のコンテンツデータの配信を受けることができる。しかも、メモリカードの認証がなされた上でコンテンツデータの配信が行われるので、システムのセキュリティおよび著作権の保護がより強化される。

[実施の形態 7]

- 15       図 44 は、実施の形態 7 における携帯電話機 107 の構成を説明するための概略ブロック図である。

- 20       図 32 に示した実施の形態 5 の携帯電話機 105 の構成と異なる点は、携帯電話機という再生装置に共通な復号鍵 Kcom を保持する Kcom 保持部 1530 と、復号処理部 1506 の出力を受けて、復号鍵 Kcom について復号し、音楽再生部 1508 にライセンスキー Kc を与える復号処理部 1532 とを備える構成となっていることである。

携帯電話機 107 のその他の点は、図 32 に示した実施の形態 5 の携帯電話機 105 の構成と同様であるので、同一部分には同一符号を付してその説明は繰り返さない。メモリカード 140 の構成も同様である。

- 25       すなわち、実施の形態 7 では、実施の形態 5 において、音楽再生部 1508 に最終的にライセンスキー Kc と与えられる以前において、システムを構成する機器間で授受されていたライセンスキー Kc を、実施の形態 7 では、さらに暗号化した [Kc] Kcom という状態でやり取りする以外は、実施の形態 5 の構成と同様である。

なお、以下の説明では、復号鍵 Kcom は共通鍵であるものとして説明する

が、本発明はこのような場合に限定されず、たとえば、暗号化は公開鍵K P c o mで行い、復号化を公開暗号化鍵K P c o mとは非対称な秘密復号鍵K c o mで行なう構成としてもよい。

図45は、実施の形態7の携帯電話機107に対応した配信サーバ13の構成を示す概略ブロック図である。図33に示した実施の形態5の配信サーバ12の構成と異なる点は、データ処理部310は、復号鍵K c o mを保持するK c o m保持部330と、配信制御部312を介して配信情報データベース304から与えられるライセンスキーK cを復号鍵K c o mにより暗号化処理して、暗号化ライセンスキー[K c] K c o mとして暗号化処理部320に与える暗号化処理部332をさらに備える構成となっている点である。

配信サーバ13のその他の点は、図33に示した実施の形態5の配信サーバ12の構成の構成と同様であるので、同一部分には同一符号を付してその説明は繰り返さない。

#### [配信モード]

図46および図47は、図44および45で説明した配信サーバ13と携帯電話機107を用いた配信モードを説明するための第1および第2のフローチャートである。

図46および図47においても、ユーザ1が、メモ리카ード140を用いることで、配信サーバ13からコンテンツデータ（音楽データ）の配信を受ける場合の動作を説明している。

ただし、図46および図47の処理は、ステップS134において、配信サーバ13が、ライセンスキーK cを配信情報データベース304より取得した後、暗号化処理部332がキーK cを暗号化して（ステップS135）、以後は、暗号化ライセンスキー[K c] K c o mとして授受される点を除いては、図35および図36で説明した実施の形態5の配信モードと同様であるので、その説明は繰り返さない。

以上のような配信モードでは、実施の形態5に比べて、さらにシステムのセキュリティが強化される。

#### [再生動作]

図４８および図４９は、携帯電話機１０７内において、メモ리카ード１４０に保持された暗号化コンテンツデータから、音楽信号を再生し、音楽として外部に出力するための再生処理を説明する第１および第２のフローチャートである。

ただし、図４８および図４９に示した再生処理は、ステップＳ２６４でメモ리카ード１４０のメモリ１４１２から読み出されるキーが、暗号化ライセンスキー〔Ｋｃ〕Ｋｃｏｍであり、以後、暗号化ライセンスキー〔Ｋｃ〕Ｋｃｏｍとして携帯電話機１０７に送信され、携帯電話機１０７において、ステップＳ２７３で復号処理部１５３２によりキー〔Ｋｃ〕Ｋｃｏｍが復号されライセンスキーＫｃが音楽再生部１５０８に与えられる点以外は、図３７および図３８に示した実施の形態５の再生処理と同様であるのでその説明は繰り返さない。

このような構成とすることで、再生モードにおけるシステムのセキュリティおよび著作権の保護が一層向上する。

〔移動または複製モード〕

図５０および図５１は、実施の形態７において、２つのメモ리카ード間において、コンテンツデータおよびキーデータ等の移動または複製を行なう処理を説明するための第１および第２のフローチャートである。

ただし、図５０および図５１の処理は、ライセンスキーＫｃが、暗号化ライセンスキー〔Ｋｃ〕Ｋｃｏｍとして授受される点を除いては、図３９および図４０で説明した実施の形態５の移動または複製モードの動作と同様であるので、その説明は繰り返さない。

このような構成とすることで、移動または複製モードにおけるシステムのセキュリティおよび著作権の保護が一層向上する。

〔実施の形態８〕

図５２は、本発明の実施の形態８のコンテンツデータ販売機３０２０の構成を示す概略ブロック図であり、実施の形態６の図４１と対比される図である。

コンテンツデータ販売機３０２０の構成が、実施の形態６のコンテンツデータ販売機３０１０の構成と異なる点は、データ処理部２１００は、復号鍵Ｋｃｏｍを保持するＫｃｏｍ保持部３３０と、配信制御部３１２を介して配信情報データベース３０４から与えられるライセンスキーＫｃを復号鍵Ｋｃｏｍにより暗号化

処理して、暗号化ライセンスキー [Kc] Kcomとして暗号化処理部320に与える暗号化処理部332をさらに備える構成となっている点である。

コンテンツデータ販売機3020のその他の点は、図41に示した実施の形態6のコンテンツデータ販売機3010の構成の構成と同様であるので、同一部分には同一符号を付してその説明は繰り返さない。

もちろん、実施の形態8でも、コネクタ2010により、携帯電話機107を介して、メモ리카ード140とコンテンツデータ販売機3020とがデータの授受を行なう構成とすることも可能である。

#### [配信モード]

図53および図54は、図52で説明したコンテンツデータ販売機3020を用いたデータ配信システムにおける配信モードを説明するための第1および第2のフローチャートである。

図53および図54においては、ユーザ1が、メモ리카ード140を用いることで、コンテンツデータ販売機3020からコンテンツデータ（音楽データ）の配信を受ける場合の動作を説明している。

ただし、図53および図54の処理は、ステップS540において、コンテンツデータ販売機3020が、ライセンスキーKcを配信情報データベース304より取得した後、暗号化処理部332がライセンスキーKcを暗号化して（ステップS541）、以後は、暗号化ライセンスキー [Kc] Kcomとして授受される点を除いては、図42および図43で説明した実施の形態5の配信動作と同様であるので、その説明は繰り返さない。

以上のような配信モードでは、実施の形態6に比べて、さらにシステムのセキュリティが強化される。

ここでは暗号化コンテンツデータを配信し、メモ리카ード110、120、140内のメモリ1412に格納した後、ライセンスキーKc、ライセンス情報データLicenseの配信を受けるように説明したが、逆にライセンスキーKc、ライセンス情報データLicenseを配信し、メモ리카ード110、120、140内のレジスタ1500に格納した後、暗号化コンテンツデータの配信を受けても構わない。



さらに、移動モードにおいても配信モードと同様に、暗号化コンテンツデータ、ライセンスキーK<sub>c</sub>、ライセンス情報データL<sub>i</sub>c<sub>e</sub>n<sub>s</sub>e<sub>e</sub>のいずれの移動が先であっても構わない。

5      なお、以上説明してきた各実施の形態において、配信データとしてコンテンツデータに付随する非暗号化データ、たとえば、上記音楽データの曲名、実演者（歌手、演奏家等）、作曲家、作詞家等の当該音楽データ（コンテンツデータ）に関する著作権情報や配信サーバ10、11、コンテンツデータ販売機3000、3001に対してアクセスするための情報等を、付加データD<sub>i</sub>として暗号化コンテンツデータと併せて配信することも可能である。この付加データD<sub>i</sub>は、配  
10   信、移動、複製においてはコンテンツデータとともに処理され、再生時には分離されてコンテンツデータとは個別にアクセス可能となるように、暗号化コンテンツデータと同じメモリ1412に格納される。

〔実施の形態9〕

15   図55は、以上説明してきたメモ리카ード110、120、140等の端子1202部分の構成を説明する概略ブロック図である。

以下では、メモ리카ード140の端子1202部分の構成であるものとして説明する。

20   メモ리카ード140には、端子1202からシリアルにデータやコマンドが与えられる。これに対して、メモ리카ード140中のデータバスB<sub>S</sub>3には、パラレルにデータやコマンドが伝達されるものとする。

図55は、このようなメモ리카ード140へのデータ入力時のシリアル・パラレル変換と、データ出力時のパラレル・シリアル変換を行なう構成を示す概略ブロック図である。

25   端子1202中のデータピン1460には、データ入出力のタイミングを指定するための信号である信号C<sub>S</sub>が与えられる。たとえば、信号C<sub>S</sub>が活性化（“L”レベル）となった後の所定期間後に、データ入力ピン1462に与えられるデータが“L”レベルとなることで、データ入力のタイミングが検出される。どうように、信号C<sub>S</sub>が活性化（“L”レベル）となった後の所定期間後に、データ出力ピン1464に出力されるデータが“L”レベルとなることで、

データ出力のタイミングが検出される。インタフェースコントローラ1490は、メモ리카ード140の外部からデータバスBS3へのデータ入力、およびデータバスBS3からメモ리카ード140外部へのデータ出力を管理する。

データ入力時は、データ入力ピン1462に与えられたデータは、バッファ1468を介して、縦列に接続されたD-フリップフロップ1470. 0~1470. 7に入力される。すなわち、8ビット分のデータが入力された時点で、D-フリップフロップ1470. 0~1470. 7の全てのデータが更新され、その時点で、インタフェースコントローラ1490により制御されて、データバッファ1427. 0~1427. 7からデータバスBS3へデータが平行に出力される。

データ出力時は、データバスBS3からのデータがマルチプレクサ1476. 1~1476. 7を介して、平行に与えられD-フリップフロップ1474. 0~1474. 7に格納される。その後インタフェースコントローラ1490により制御されて、マルチプレクサ1476. 1~1476. 7の接続が切り換えられ、D-フリップフロップ1474. 0~1474. 7が縦列に接続される。この状態で、D-フリップフロップ1474. 0~1474. 7のそれぞれに格納されたデータが、順次シリアルに、インタフェースコントローラ1490により制御される出力バッファ1470を介して、データ出力ピン1464から出力される。

#### 20 [実施の形態9の変形例]

図56は、データ入力の速度を向上させるために、データ入力ピンの本数を1本から2本または4本に可変とすることが可能な、メモ리카ード140の端子1202部分の構成の変形例を説明するための概略ブロック図である。

図55に示した構成と異なる点は、まず、4本のデータ入力ピン1462. 0~1462. 3およびそれらに対応する入力バッファ1468. 0~1468. 3が設けられていることと、これらデータ入力ピン1462. 0~1462. 3に与えられたコマンドを入力バッファ1468. 0~1468. 3からインタフェースコントローラ1490に伝達するためのマルチプレクサ1467と、データ入力ピン1462. 0~1462. 3に与えられたデータまたはコマンドを、入力

バッファ1468. 0~1468. 3からD-フリップフロップ1470. 0~1470. 7に選択的に与えるためのマルチプレクサ1469. 1~1469. 7とをさらに備える構成となっていることである。

次に動作について簡単に説明する。

- 5 電源投入後には、たとえば、メモ리카ード140は、1本のデータ入力ピン1462. 0からのみデータ入力を受けつける状態となっている。

- 以下では、外部からデータ入力ピン1462. 0~1462. 3およびマルチプレクサ1467を経由してインタフェースコントローラ1490に与えられたコマンドにより、インタフェースコントローラ1490がマルチプレクサ1469. 1~1469. 7を制御することで、4本のデータ入力ピン1462. 0~1462. 3からのデータをパラレルに入力するモードに動作モードが変更されたものとする。

- まず、第1のタイミングで4本のデータ入力ピン1462. 0~1462. 3に与えられたデータは、マルチプレクサ1469. 1~1469. 3を経由して  
15 D-フリップフロップ1470. 0~1470. 3に与えられる。

- 次の第2のタイミングで、マルチプレクサ1469. 1~1469. 7の接続が切り替わり、D-フリップフロップ1470. 0~1470. 3の出力がそれぞれ、D-フリップフロップ1470. 4~1470. 7に与えられて格納される。さらに第3のタイミングで、4本のデータ入力ピン1462. 0~1462. 3に与えられたデータは、マルチプレクサ1469. 1~1469. 3を経由してD-フリップフロップ1470. 0~1470. 3に与えられる。  
20

- 以上で、8ビット分のデータのD-フリップフロップ1470. 0~1470. 7への格納が終了する。以後は、図55の場合と同様に、データバスBS3に対してパラレルに8ビット分のデータが与えられる。

- 25 データ出力の際の動作は、図55の場合と同様である。

以上のような構成により、データ配信時、特にコンテンツデータ販売機2000等からコンテンツデータを購入する際のメモ리카ード140へのデータ配信時間を短縮することが可能である。

また、以上説明した各実施の形態のうち、2つの携帯電話にそれぞれ装着され

た2つのメモリカード間で、たとえば、PHSのトランシーバモード等を利用することにより、コンテンツデータの移動を行なう処理を説明した実施の形態においては、このような構成に限定されず、たとえば、1つの携帯電話機に複数のメモリカードが同時装着可能な場合は、当該携帯電話機に2つのメモリカードを同時に装着することで、コンテンツデータの移動を行なう構成とすることも可能である。このようなコンテンツデータの移動の場合は、以上説明した各実施の形態において、2つの携帯電話機間での送受信のやりとりを省略すればよい。

また、以上説明した各実施の形態では、ライセンスキーK<sub>c</sub>は暗号化された状態で、メモリ1412に格納されるものとして説明したが、ライセンスキーK<sub>c</sub>は、復号された平文の状態レジスタ1500に格納されるものとしてもよい。このような構成としても、レジスタ1500は、TRM領域内に設けられ、外部からライセンスキーK<sub>c</sub>を読み出すことはできないからである。

さらに、以上説明した各実施の形態では、暗号化コンテンツデータ[D<sub>c</sub>]K<sub>c</sub>やライセンスキーK<sub>c</sub>を格納するのは、携帯電話機100等に着脱可能なメモリカードであるものとしたが、このようなメモリカードと同等の機能を有する回路を携帯電話機内に作り込む構成としてもよい。この場合は、メモリカードの種類やメモリカードごとに規定されていた鍵は、このようにして作り込まれる回路の種類やこの回路ごとに規定されるものとすればよい。

この発明を詳細に説明し示してきたが、これは例示のためのみであって、限定となつてはならず、発明の精神と範囲は添付の請求の範囲によってのみ限定されることが明らかに理解されるであろう。

## 請求の範囲

1. コンテンツデータ供給装置から、暗号化コンテンツデータを複数のユーザの各端末に配信するためのデータ配信システムであって、

5 前記コンテンツデータ供給装置(10)は、

外部との間でデータを授受するための第1のインタフェース部(350)と、

前記暗号化コンテンツデータの通信ごとに更新される第1の共通鍵を生成する第1のセッションキー発生部(314)と、

10 前記ユーザの端末に対応して予め定められた第1の公開暗号化鍵により前記第1の共通鍵を暗号化して前記第1のインタフェース部に与えるためのセッションキー暗号化部(316)と、

前記第1の共通鍵により暗号化されて返信されるデータを復号するためのセッションキー復号部(318)と、

15 前記暗号化コンテンツデータを復号するためのライセンスキーを、前記セッションキー復号部により復号されたデータを鍵データとして暗号化するための第1のライセンスデータ暗号化処理部(320)と、

前記第1のライセンスデータ暗号化処理部の出力を第2の共通鍵でさらに暗号化して前記第1のインタフェース部に与え配信するための第2のライセンスデータ暗号化処理部(322)とを備え、

20 各前記端末(100)は、

外部との間でデータを授受するための第2のインタフェース部と、

前記暗号化コンテンツデータを受けて格納する配信データ解読部(110)とを備え、

前記配信データ解読部は、

25 前記第1の公開暗号化鍵によって暗号化されたデータを復号化するための第1の秘密復号鍵を保持する第1の鍵保持部(1402)と、

前記第1の公開暗号化鍵によって暗号化された前記第1の共通鍵を受けて、復号処理するための第1の復号処理部(1404)と、

第2の公開暗号化鍵を保持するための第2の鍵保持部(1405)と、

前記第2の公開暗号化鍵を、前記第1の共通鍵に基づいて暗号化し、前記第2のインタフェース部に出力するための第1の暗号化処理部（1406）と、

前記第2のライセンスデータ暗号化処理部からの暗号化されたライセンスキーを受け、前記第2の共通鍵に基づいて復号化するための第2の復号処理部（1410）と、

前記ライセンスキーに基づいて復号できる前記暗号化コンテンツデータを格納するための第1の記憶部（1412）と、

前記第2の公開暗号化鍵によって暗号化されたデータを復号化するための第2の秘密復号鍵を保持する第3の鍵保持部（1415）と、

前記第2の復号処理部での復号結果に基づいて、前記第2の秘密復号鍵により前記ライセンスキーを復号するための第3の復号処理部（1416）とを備える、データ配信システム。

2. 前記配信データ解読部は、前記端末に着脱可能なメモリカードであり、

前記第1の秘密復号鍵は、前記メモリカードの種類に対応して予め定められた鍵であり、

前記第2の秘密復号鍵は、前記メモリカードごとに異なる、請求項1記載のデータ配信システム。

3. 前記第1の秘密復号鍵は、前記配信データ解読部の種類に対応して予め定められた鍵であり、

前記第2の秘密復号鍵は、前記配信データ解読部ごとに異なる、請求項1記載のデータ配信システム。

4. 前記第2および第3の復号処理部は、前記コンテンツデータ供給装置において前記第2の公開暗号化鍵で暗号化され、さらに前記第2の共通鍵で暗号化されて、前記ライセンスキーとともに配信されるライセンス情報データを前記第2のインタフェース部を介して受け、前記第2の共通鍵および前記第2の秘密復号鍵に基づいて復号し、

前記配信データ解読部は、

復号された前記ライセンス情報データを格納する第2の記憶部（1500）をさらに備える、請求項2記載のデータ配信システム。

5. 前記第2の記憶部は、前記第3の復号処理部により復号された前記ライセンスキーをさらに格納する、請求項4記載のデータ配信システム。
6. 前記第1の共通鍵と前記第2の共通鍵とは、前記暗号化コンテンツデータの通信の際に、前記第1のセッションキー発生部により生成された同一の鍵データ
- 5 である、請求項4記載のデータ配信システム。
7. 前記配信データ解読部は、
- 外部から指示される再生動作モードに応じて、前記第2の記憶部に格納されたライセンス情報データにより再生可能かを判断して、前記配信データ解読部の動作を制御するための制御部をさらに備え、
- 10 前記第1の暗号化処理部は、前記制御部に制御されて、前記コンテンツデータの再生動作が指示されるのに応じて、前記第3の復号処理部からの前記ライセンスキーを受けて、第3の共通鍵に基づいて暗号化して出力し、
- 前記第1の記憶部は、前記制御部に制御されて、前記コンテンツデータの再生動作が指示されるのに応じて、前記暗号化コンテンツデータを出力し、
- 15 各前記端末は、
- 前記暗号化コンテンツデータの通信ごとに更新される前記第3の共通鍵を生成する第2のセッションキー発生部（1502）と、
- 前記配信データ解読部からの前記第3の共通鍵により暗号化された前記ライセンスキーを受けて復号して抽出し、前記第1の記憶部から出力された前記暗号化
- 20 コンテンツデータを前記ライセンスキーにより復号して再生するコンテンツデータ再生部（1506、1508）とをさらに備える、請求項6記載のデータ配信システム。
8. 前記配信データ解読部は、
- 外部から指示される他の端末に前記暗号化コンテンツデータおよび前記ライセンス情報データを移転するための移動動作モードに応じて、前記配信データ解読部の動作を制御するための制御部（1420）と、
- 25 第3の公開暗号化鍵で暗号化処理を行なうための第2の暗号化処理部（1414）とをさらに含み、
- 前記第2の復号処理部は、前記制御部に制御されて、前記移動動作モードが指

定されるのに応じて、前記第 3 の共通鍵に基づいて暗号化されて前記他の端末の側から送信される前記第 3 の公開暗号化鍵を復号して抽出し、

5 前記第 2 の暗号化処理部は、前記移動動作モードが指定されるのに応じて、前記ライセンスキーおよび前記ライセンス情報データを前記第 3 の公開暗号化鍵で暗号化し、

前記第 1 の暗号化処理部は、前記第 2 の暗号化処理部の出力を受けて、前記第 3 の共通鍵に基づいて暗号化して前記第 2 のインタフェース部に与え、

前記制御部は、前記移動動作モードが指定されるのに応じて、前記第 2 の記憶部に格納されている前記ライセンス情報データを消去し、

10 前記第 1 の記憶部は、前記移動動作モードが指定されるのに応じて、前記暗号化コンテンツデータを前記第 2 のインタフェース部に与える、請求項 7 記載のデータ配信システム。

9. 前記配信データ解読部は、

15 外部から指示される他の端末に前記暗号化コンテンツデータを移転するための複製動作モードに応じて、前記配信データ解読部の動作を制御するための制御部をさらに含み、

前記第 1 の記憶部は、前記複製動作モードが指定されるのに応じて、前記暗号化コンテンツデータを前記第 2 のインタフェース部に与える、請求項 7 記載のデータ配信システム。

20 10. 前記配信データ解読部は、

前記第 2 の共通鍵を生成するための第 3 のセッションキー発生部（1432）と、

25 前記第 3 のセッションキー発生部の出力を暗号化して前記第 2 のインタフェース部に与えることが可能な第 3 の暗号化処理部（1430）とをさらに含む、請求項 4 記載のデータ配信システム。

11. 前記配信データ解読部は、

外部から指示される再生動作モードに応じて、前記第 2 の記憶部に格納されたライセンス情報データにより再生可能かを判断して、前記配信データ解読部の動作を制御するための制御部をさらに備え、



前記第3の暗号化処理部は、第4の公開暗号化鍵により前記第3のセッションキー発生部の出力を暗号化して前記第2のインタフェース部に与え、

- 5 前記第1の暗号化処理部は、前記制御部に制御されて、前記コンテンツデータの再生動作が指示されるのに応じて、前記第3の復号処理部からの前記ライセンスキーを受けて、第3の共通鍵に基づいて暗号化して出力し、

前記第1の記憶部は、前記制御部に制御されて、前記コンテンツデータの再生動作が指示されるのに応じて、前記暗号化コンテンツデータを出力し、

各前記端末は、

- 10 前記暗号化コンテンツデータの通信ごとに更新される前記第3の共通鍵を生成する第2のセッションキー発生部（1502）と、

前記第4の公開暗号化鍵を前記配信データ解読部に与える公開鍵保持部（1524）と、

前記第4の公開暗号化鍵で暗号化された前記第2の共通鍵を復号可能な公開鍵復号部（1522）と、

- 15 前記配信データ解読部からの前記第3の共通鍵により暗号化された前記ライセンスキーを受けて復号して抽出し、前記第1の記憶部から出力された前記暗号化コンテンツデータを前記ライセンスキーにより復号して再生するコンテンツデータ再生部（1506、1508）とをさらに備える、請求項10記載のデータ配信システム。

- 20 12. 前記配信データ解読部は、

外部から指示される他の端末に前記暗号化コンテンツデータおよび前記ライセンス情報データを移転するための移動動作モードに応じて、前記配信データ解読部の動作を制御するための制御部と、

- 25 第3の公開暗号化鍵で暗号化処理を行なうための第2の暗号化処理部とをさらに含み、

前記第2の復号処理部は、前記制御部に制御されて、前記移動動作モードが指定されるのに応じて、前記第3の共通鍵に基づいて暗号化されて前記他の端末の側から送信される前記第3の公開暗号化鍵を復号して抽出し、

前記第2の暗号化処理部は、前記移動動作モードが指定されるのに応じて、前

記ライセンスキーおよび前記ライセンス情報データを前記第 3 の公開暗号化鍵で暗号化し、

前記第 1 の暗号化処理部は、前記第 2 の暗号化処理部の出力を受けて、前記第 3 の共通鍵に基づいて暗号化して前記第 2 のインタフェース部に与え、

- 5 前記制御部は、前記移動動作モードが指定されるのに応じて、前記第 2 の記憶部に格納されている前記ライセンス情報データを消去し、

前記第 1 の記憶部は、前記移動動作モードが指定されるのに応じて、前記暗号化コンテンツデータを前記第 2 のインタフェース部に与える、請求項 11 記載のデータ配信システム。

- 10 13. 前記配信データ解読部は、

外部から指示される他の端末に前記暗号化コンテンツデータを移転するための複製動作モードに応じて、前記配信データ解読部の動作を制御するための制御部をさらに含み、

- 15 前記第 1 の記憶部は、前記複製動作モードが指定されるのに応じて、前記暗号化コンテンツデータを前記第 2 のインタフェース部に与える、請求項 11 記載のデータ配信システム。

14. 前記第 1 のインタフェース部と前記第 2 のインタフェース部とは、携帯電話網により接続され、

前記コンテンツデータ供給装置は、

- 20 前記第 1 の公開暗号鍵に基づいて、前記ユーザの認証を行なう、請求項 1 記載のデータ配信システム。

15. 前記第 1 のインタフェース部は、

前記端末と直接接続可能なコネクタ部 (2010) を含む、請求項 1 記載のデータ配信システム。

- 25 16. 前記第 1 のインタフェース部は、

前記メモリーカードと直接接続可能な接続部 (2030) を含む、請求項 2 記載のデータ配信システム。

17. コンテンツデータ供給装置から、暗号化コンテンツデータと前記暗号化データを復号するためのライセンスキーとのうちの少なくとも 1 つを複数のユーザ

- の各端末に配信するためのデータ配信システムであって、
- 前記コンテンツデータ供給装置は、
- 外部との間でデータを授受するための第1のインタフェース部（350）と、
- 前記暗号化コンテンツデータの通信ごとに更新される第1の共通鍵を生成する
- 5 第1のセッションキー発生部（314）と、
- 前記ユーザの端末に対応して予め定められた第1の公開暗号化鍵により前記第1の共通鍵を暗号化して前記第1のインタフェース部に与えるためのセッションキー暗号化処理部（316）と、
- 前記第1の共通鍵により暗号化されて返信される第2の共通鍵と第2の公開暗
- 10 号化鍵を復号し抽出するセッションキー復号部（318）と、
- 前記暗号化コンテンツデータを復号するためのライセンスキーを、前記セッションキー復号部により復号された前記第2の公開暗号化鍵により暗号化するための第1のライセンスデータ暗号化処理部（320）と、
- 前記第1のライセンスデータ暗号化処理部の出力を前記第2の共通鍵でさらに
- 15 暗号化して前記第1のインタフェース部に与え配信するための第2のライセンス暗号化処理部（322）とを備え、
- 各前記端末は、
- 外部との間でデータを授受するための第2のインタフェース部と、
- 前記暗号化コンテンツデータおよび前記ライセンスキーを受けて格納する配信
- 20 データ解読部（140）とを備え、
- 前記配信データ解読部は、
- 前記第1の公開暗号化鍵によって暗号化されたデータを復号化するための第1の秘密復号鍵を保持する第1の鍵保持部（1402）と、
- 前記第1の公開暗号化鍵によって暗号化された前記第1の共通鍵を受けて、復
- 25 号処理するための第1の復号処理部（1404）と、
- 前記第2の公開暗号化鍵を保持するための第2の鍵保持部（1405）と、
- 前記第2の共通鍵を生成する第2のセッションキー発生部（1432）と、
- 前記第2の公開暗号化鍵と前記第2の共通鍵を、前記第1の共通鍵に基づいて暗号化し、前記第2のインタフェース部に出力するための第1の暗号化処理部

(1406)と、

前記第2のライセンスデータ暗号化処理部からの暗号化されたライセンスキーを受け、前記第2の共通鍵に基づいて復号するための第2の復号処理部(1410)と、

- 5 前記ライセンスキーにて復号可能な暗号化コンテンツデータを格納するための記憶部と、

前記第2の公開暗号化鍵によって暗号化されたデータを復号化するための第2の秘密復号鍵を保持する第3の鍵保持部(1415)と、

- 10 前記第2の復号処理部の復号結果に基づいて、前記第2の秘密復号鍵により前記ライセンスキーを復号し抽出するための第3の復号処理部(1416)と、

前記第1の公開暗号化鍵を少なくとも含む第1の認証データを公開認証鍵により復号できるように暗号化して保持し外部に出力可能な第1の認証データ保持部(1442)とを備え、

前記コンテンツデータ供給装置は、

- 15 前記公開認証鍵により復号でき、かつ外部から与えられる前記第1の認証データを復号して抽出するための第1の認証復号処理部(326)と

前記第1の認証復号処理部により抽出された前記第1の認証データに基づいて認証処理を行ない、少なくともライセンスキーを配信するか否かを判断する配信制御部(312)をさらに含む、データ配信システム。

- 20 18. 前記記憶部は、

前記第2の復号処理部により復号された結果、前記第2の秘密復号鍵により復号可能な状態の前記ライセンスキーと前記暗号化コンテンツデータとを格納するための第1の記憶手段(1412)を含む、請求項17記載のデータ配信システム。

- 25 19. 前記記憶部は、

前記暗号化コンテンツデータを格納するための第1の記憶手段(1412)と、

前記第3の復号処理部により復号された前記ライセンスキーを格納するための第2の記憶手段(1500)とを含む、請求項17記載のデータ配信システム。

20. 前記配信データ解読部は、前記端末に着脱可能なメモリカードであり、  
前記第1の秘密復号鍵は、前記メモリカードの種類に対応して予め定められた値であり
- 5 前記第2の秘密復号鍵は、前記メモリカードごとに異なる、請求項17記載のデータ配信システム。
21. 前記第1の秘密復号鍵は、前記配信データ解読部の種類に対応して予め定められた値であり
- 前記第2の秘密復号鍵は、前記配信データ解読部ごとに異なる、請求項17記載のデータ配信システム。
- 10 22. 各前記端末は、コンテンツ再生部をさらに備え、  
前記コンテンツ再生部は、  
予め定められた第3の公開暗号鍵を少なくとも含む第2の認証データを前記公開認証鍵に基づいて復号できるように暗号化して保持し、外部に対して出力できる第2の認証データ保持部（1525）をさらに含む、請求項17記載のデータ
- 15 配信システム。
23. 前記第1の認証復号処理部は、  
前記公開認証鍵により復号できるように暗号化された前記第2の認証データをさらに復号して出力し、  
前記配信制御部は、
- 20 前記第1の認証復号処理部にて抽出された前記第1の認証データおよび前記第2の認証データに基づいて認証処理を行ない、少なくともライセンスキーを配信するか否かを判断する、請求項22に記載のデータ配信システム。
24. 前記第1のインタフェース部と前記第2のインタフェース部とは、携帯電話網により接続される、請求項17記載のデータ配信システム。
- 25 25. 前記第1のインタフェース部は、  
前記端末と直接接続可能なコネクタ部を含む、請求項17記載のデータ配信システム。
26. 前記第1のインタフェース部は、  
前記データ格納部と直接接続可能な接続部を含む、請求項20記載のデータ配

信システム。

27. 前記配信データ解読部は、

前記接続部からのデータを受ける複数の端子（1462.0-1462.3）を含み、

- 5 外部からの指令に従って、前記接続部からデータを受ける端子数が切換え可能である、請求項26記載のデータ配信システム。

28. 前記記憶部は、前記第2の復号処理部の出力を受けて、前記第2の秘密復号鍵により復号可能なように暗号化されている前記ライセンスキーを格納し、

前記コンテンツ再生部は、

- 10 前記第3の公開暗号鍵にて暗号化されたデータを復号する第3の秘密復号鍵を保持するための第4の鍵保持部（1520）と、

外部にて前記第3の公開暗号化鍵によって暗号化された第2の共通鍵を復号し抽出するための第4の復号処理部（1522）と、

第3の共通鍵を生成する第3のセッションキー発生部（1502）と、

- 15 前記第4の復号処理部にて復号し抽出した前記第2の共通鍵に基づいて、前記第3の共通鍵を暗号化し出力するための第2の暗号化処理部（1504）と、

前記コンテンツ再生部の外部にて前記第3の共通鍵に基づいて暗号化されたライセンスキーを復号し抽出するための第5復号処理部（1506）と、

- 20 前記記憶部に記録された暗号化コンテンツデータを、抽出した前記ライセンスキーにて復号し、再生するためのデータ再生部（1508）とをさらに備え、

前記配信データ解読部は、

前記公開認証鍵により復号できる前記コンテンツ再生部からの与えられる暗号化された前記第2の認証データを復号して前記第3の公開暗号化鍵を抽出するための第2の認証復号処理部（1452）と、

- 25 前記第2のセッションキー発生部にて生成した前記第2の共通鍵を前記第3の公開暗号化鍵に基づいて暗号化する第3の暗号化処理部（1430）と、

前記コンテンツ再生部にて前記第2の共通鍵にて暗号化された前記第3の共通鍵を受けて、前記第2の復号処理部（1410）にて前記第2の共通鍵に基づいて復号した前記第3の共通鍵に基づいて、前記記憶部に格納されたデータを前記

第2の秘密復号鍵にて復号した前記ライセンスキーを、前記第1の暗号化処理部にて暗号化し、前記コンテンツ再生部へ出力を指示する制御部（1420）とをさらに備え、

5 前記制御部は、前記第2の認証復号処理部により復号された前記第2の認証データに基づいて認証処理を行ない、少なくともライセンスキーを出力するか否かを判断する、請求項22記載のデータ配信システム。

29. 前記記憶部は、前記第2の復号処理部の出力を受けて、前記第2の秘密復号鍵により復号可能なように暗号化されている前記ライセンスキーを格納し、

前記配信データ解読部は、

10 他の端末の配信データ解読部に対して少なくとも前記ライセンスキーを移転するために、前記配信データ解読部の外部から指示される移動処理に応じて、前記他の配信データ解読部からの前記公開認証鍵によって復号できる暗号化された第1の認証データを、前記公開認証鍵にて復号して、前記他の配信データ解読部における前記第1の公開暗号化鍵を抽出する第2の認証復号処理部（1452）と、  
15 と、

前記他の配信データ解読部の前記第1の公開暗号化鍵によって前記第2の共通鍵を暗号化するための第3の暗号化処理部（1430）と、

前記他の配信データ解読部の第2の公開暗号化鍵による暗号化処理を行うための第4の暗号化処理部（1414）とをさらに含み、

20 前記第2のセッションキー発生部は、前記移動処理に応じて、前記第2の共通鍵を発生し、

前記第2の復号処理部は、前記移動処理に応じて、前記他の配信データ解読部から前記第2の共通鍵によって暗号化され、入力される第4の共通鍵と前記他の配信データ解読部の第2の公開暗号化鍵とを復号して抽出し、

25 前記第3の復号処理部は、前記移動処理に応じて、前記第2の秘密復号鍵に基づいて、前記記憶部に格納された前記第2の公開暗号化鍵にて暗号化されたデータを復号して、ライセンスキーを抽出し、

前記第4の暗号化処理部は、前記移動処理に応じて、前記他の配信データ解読部の第2の公開暗号化鍵に基づいて、抽出された前記ライセンスキーを暗号化

し、

前記第 1 の暗号化処理部は、前記移動処理に応じて、前記第 4 の暗号化処理部の出力を前記第 4 の共通鍵にて暗号化し、前記他の配信データ解読部に対して出力し、

- 5 前記制御手段は、前記第 2 の認証復号処理部により抽出された前記他のデータ解読部から出力された第 2 の認証データに基づき認証処理を行ない、少なくともライセンスキーを出力するか否かを判断する、請求項 20 記載のデータ配信システム。

30. 前記他の配信データ解読部は、

- 10 前記認証復号処理においては、前記配信データ解読部から少なくとも前記ライセンスキーを移転するための前記他の配信データ解読部の外部から指示される移動処理に応じて、前記第 1 の認証データ保持部が前記第 1 の認証データを出力し、

- 15 前記第 1 の復号処理部は、前記移動処理に応じて、前記配信データ解読部から前記第 1 の公開暗号化鍵によって暗号化され、入力される前記配信データ解読部にて発生された前記第 2 の共通鍵を復号して抽出し、

前記第 2 のセッションキー発生部は、前記移動受理処理に応じて、前記第 4 の共通鍵を発生し、

- 20 前記第 1 の暗号化処理部は、前記移動受理処理に応じて、第 2 の共通鍵に基づいて、前記第 2 の公開暗号化鍵と前記第 4 の共通鍵とを暗号化して出力し、

前記第 2 の復号処理部は、前記配信データ解読部において前記第 2 の公開暗号化鍵にて暗号化され、さらに前記第 4 の共通鍵にて暗号化されたライセンスキーを前記第 4 の共通鍵にて復号し、前記記憶部に記録する請求項 29 記載のデータ配信システム。

- 25 31. 前記コンテンツデータ供給装置は、

前記コンテンツ再生部と共通な第 5 の共通鍵を保持する第 5 の鍵保持部と、

前記第 5 の鍵保持部に保持された前記第 5 の共通鍵に基づいて、前記ライセンスキーを暗号化し前記第 1 のライセンス暗号化処理部に対して出力する第 3 のライセンス暗号化部をさらに含み、



前記コンテンツ再生部は、

前記第 5 の共通鍵を保持する第 6 の鍵保持手段と、

- 5 前記第 4 の復号処理部と前記データ再生部との間に設けられ、前記第 6 の鍵保持部に保持された前記第 5 の共通鍵によって、前記第 4 の復号処理部の出力から前記ライセンスキーを復号し抽出し、前記データ再生部に対して出力する第 5 の復号処理部をさらに含む、請求項 26 記載のデータ配信システム。

32. 前記コンテンツデータ供給装置は、

前記コンテンツ再生部にて復号可能な第 4 の公開暗号化鍵を保持する第 5 の鍵保持部と、

- 10 第 4 の公開暗号化鍵に基づいて前記ライセンスキーを暗号化し前記第 1 のライセンス暗号化処理部にて出力する第 3 のライセンス暗号化部をさらに含む、

前記コンテンツ再生部は、

第 4 の公開暗号化鍵によって暗号化されたデータを復号できる第 4 の秘密復号鍵を保持する第 6 の鍵保持手段と、

- 15 前記第 4 の復号処理部と前記データ再生部との間に設けられ、第 4 の秘密復号鍵によって前記第 4 の復号処理部の出力から前記ライセンスキーを復号し抽出し、前記データ再生部に対して出力する第 5 の復号処理部をさらに含む、請求項 26 記載のデータ配信システム。

33. 前記端末は、

- 20 複数の配信データ解読部を備える、請求項 20 記載のデータ配信システム。

FIG.1

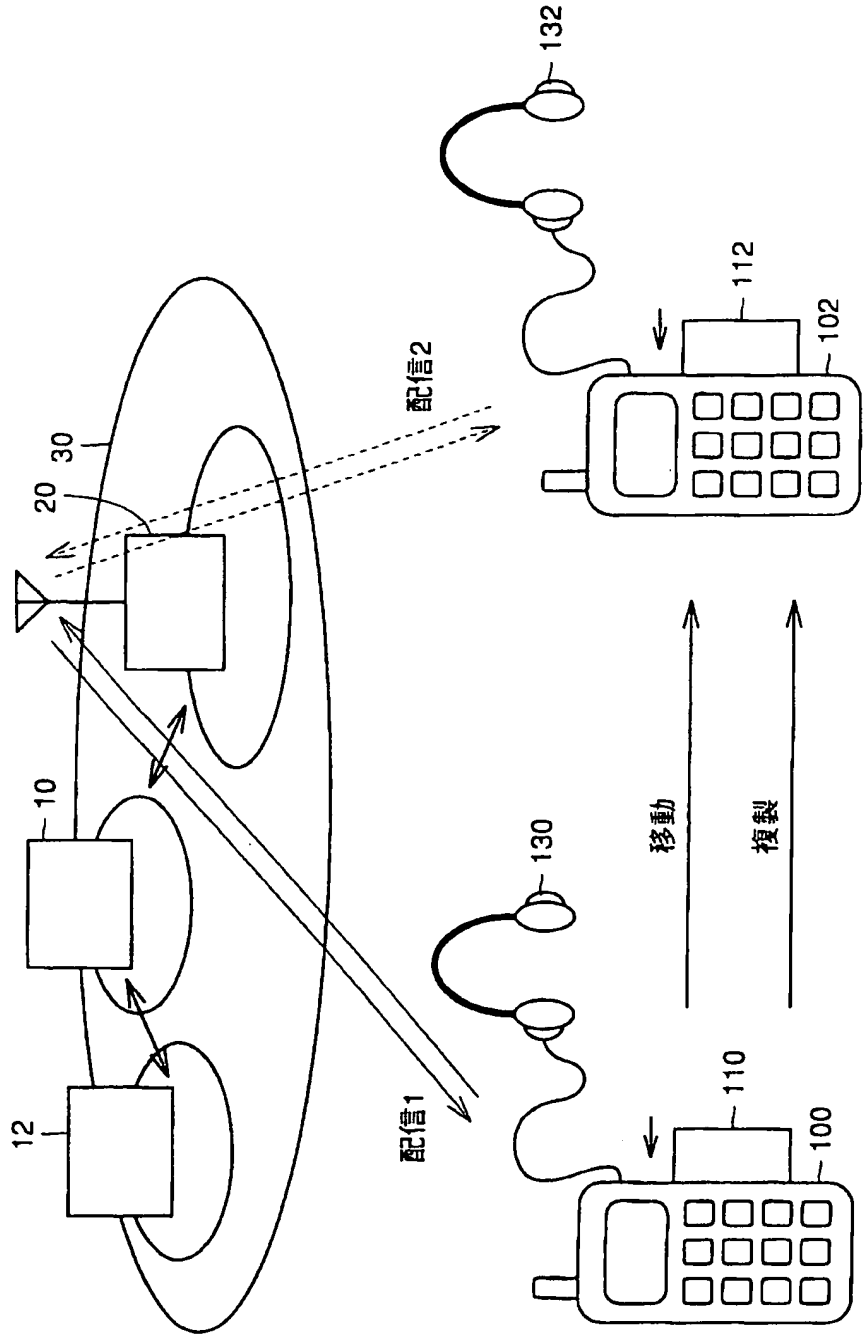


FIG.2

	記号	属性	特性	
			媒体固有	メモリカードの種類ごとに固有な情報を有する
メモリカード内 管理の鍵	Kmedia(n)	秘密復号鍵		メモリカード毎に異なる
	Kcard(n)	秘密復号鍵		
	KPcard(n)	公開暗号化鍵		Kcard(n)と対を成す。 KPcard(n)により暗号化されたデータは、Kcard(n)で復号可能
メモリカード外 管理の鍵	KPmedia(n)	公開暗号化鍵	媒体固有	Kmediaと対を成す。 KPmediaにより暗号化されたデータは、Kmediaで復号可能。
	Ks	共通鍵	セッション 固有	通信毎 (例：アクセス毎) に発生。 配信サーバ、携帯電話機にて管理
	Kc	共通鍵	ライセン スキー	暗号化コンテンツデータの復号鍵
配信データ	License-ID	再生に関する 情報		例：曲目の特定情報 再生回数の制限情報
	User-ID	受信者を識別 する情報		例：電話番号
	Dc	コンテンツ データ		例：音楽
	[Dc]Kc	暗号化コン テンツデータ		共通鍵Kcにより暗号化されたコンテンツデータ

FIG.3

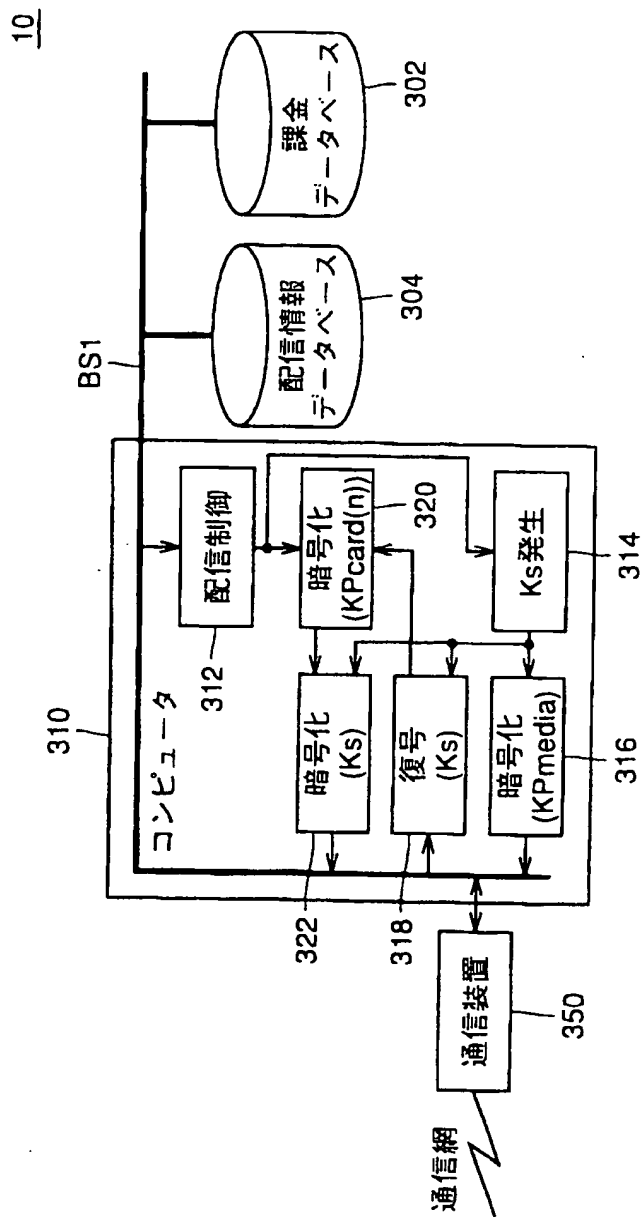


FIG.4

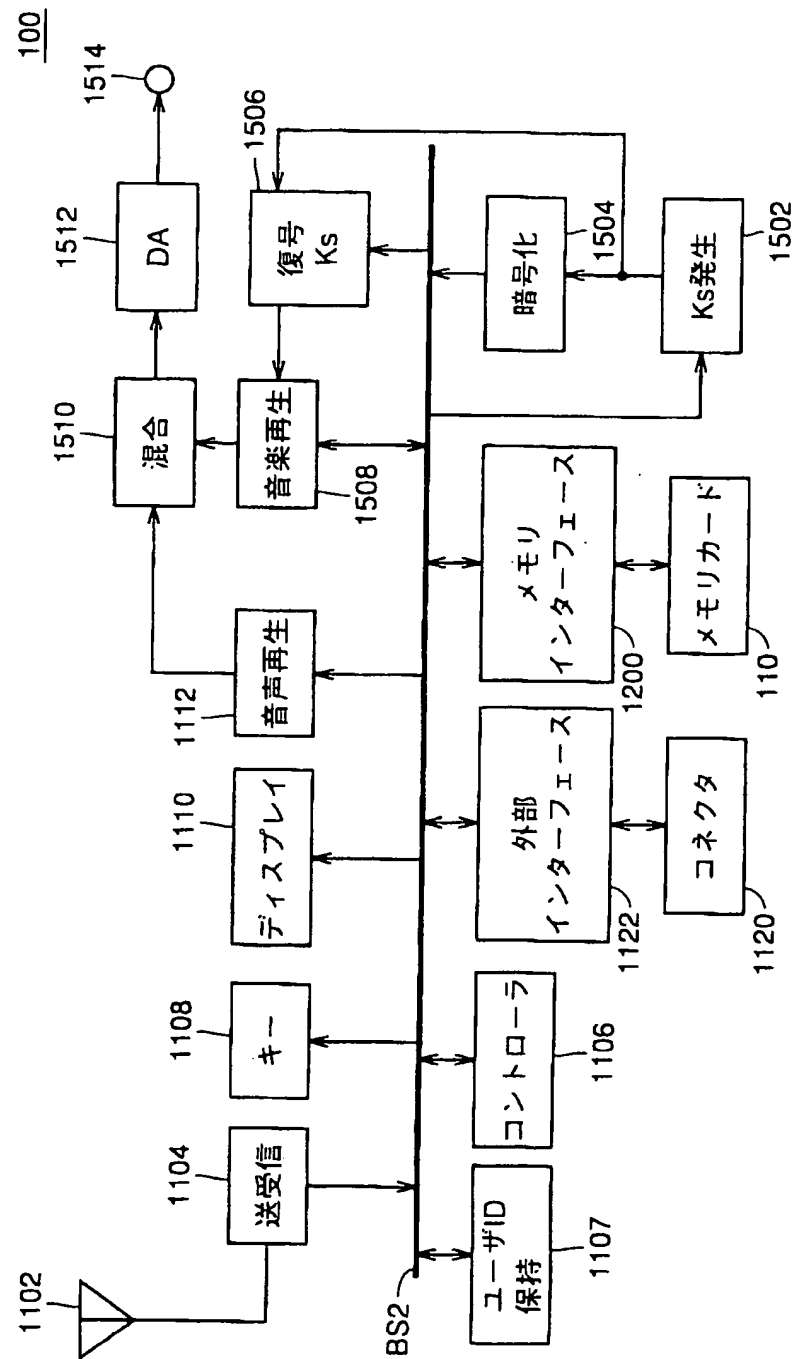


FIG.5

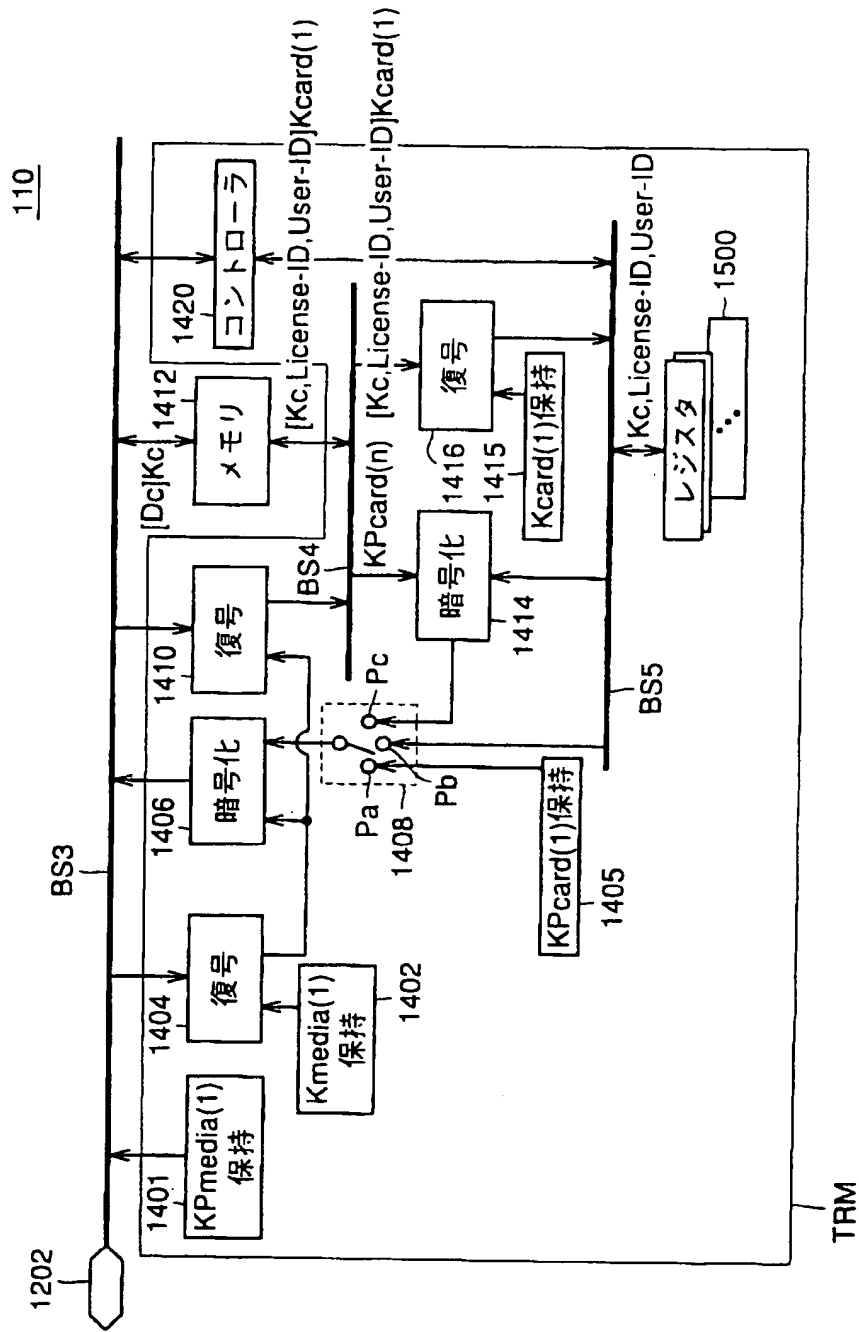


FIG. 6

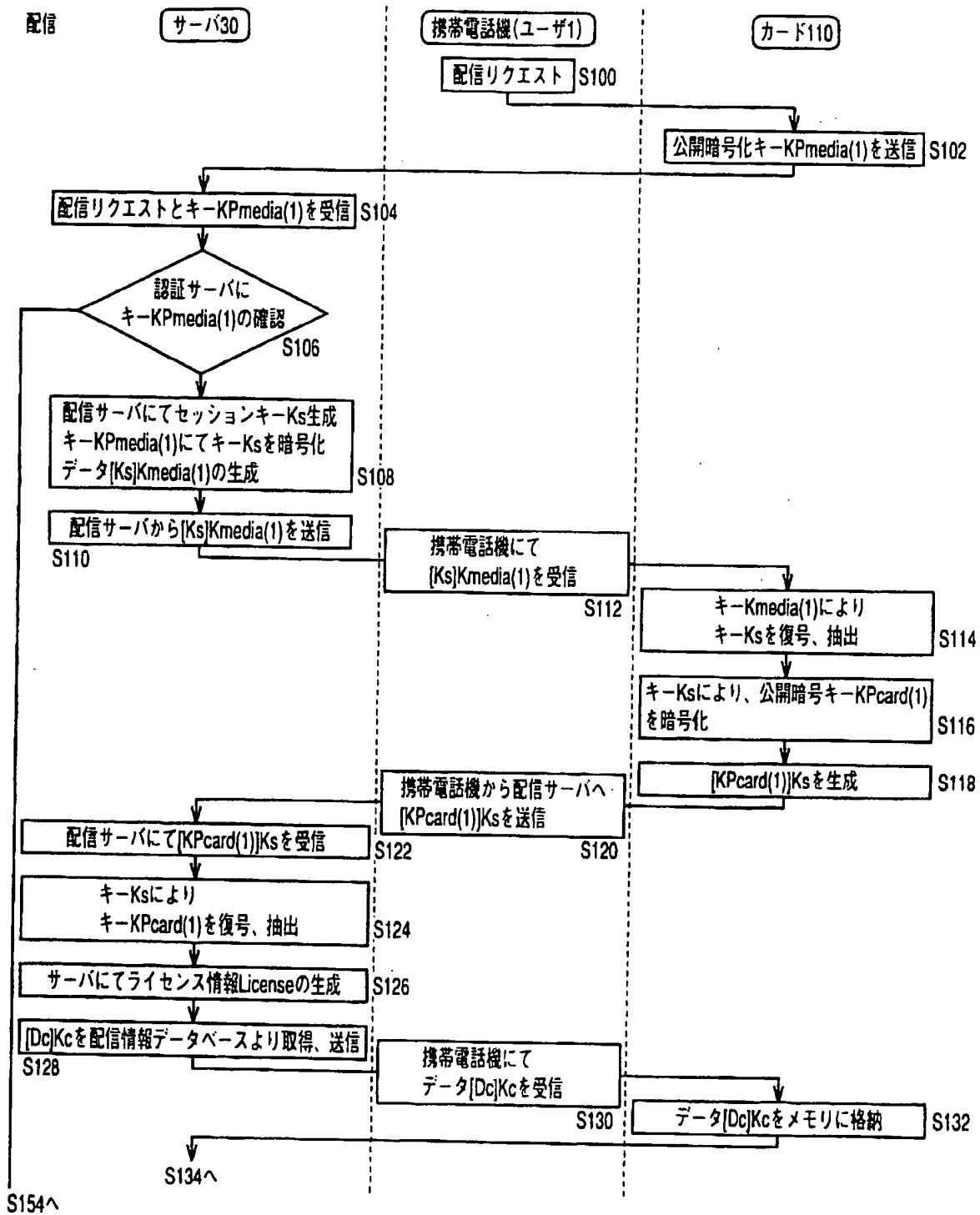


FIG. 7

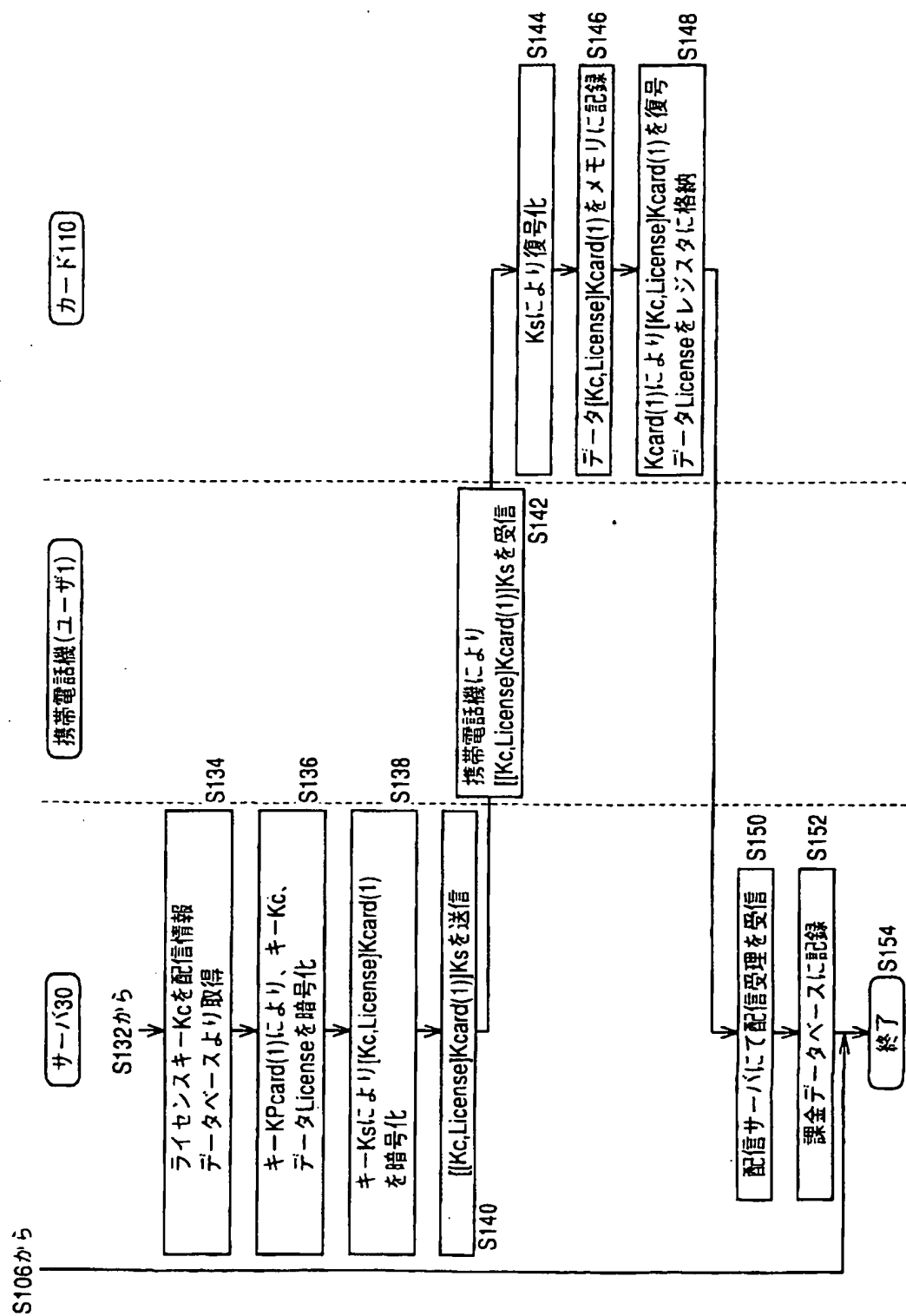




FIG.8

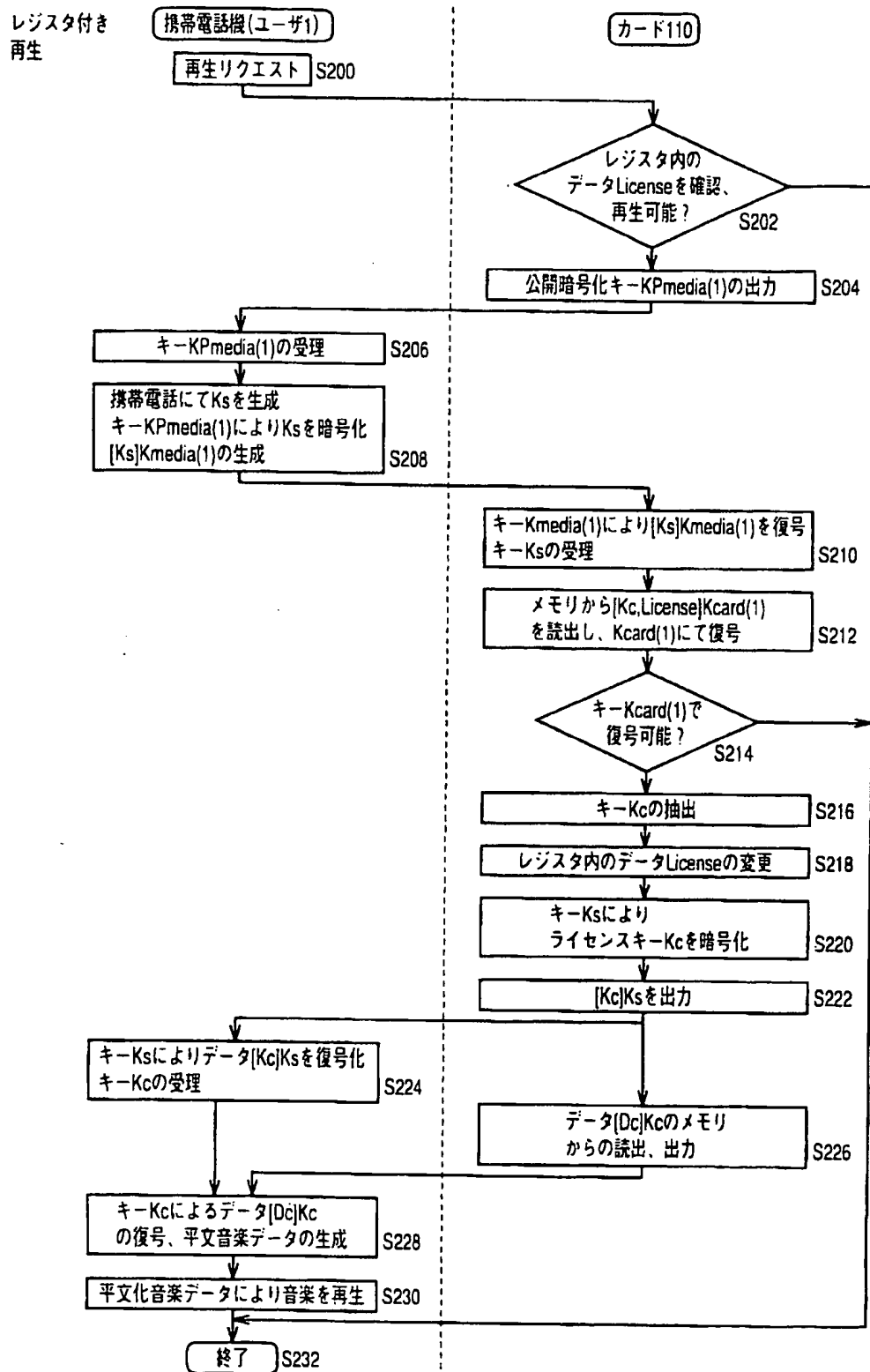


FIG.9

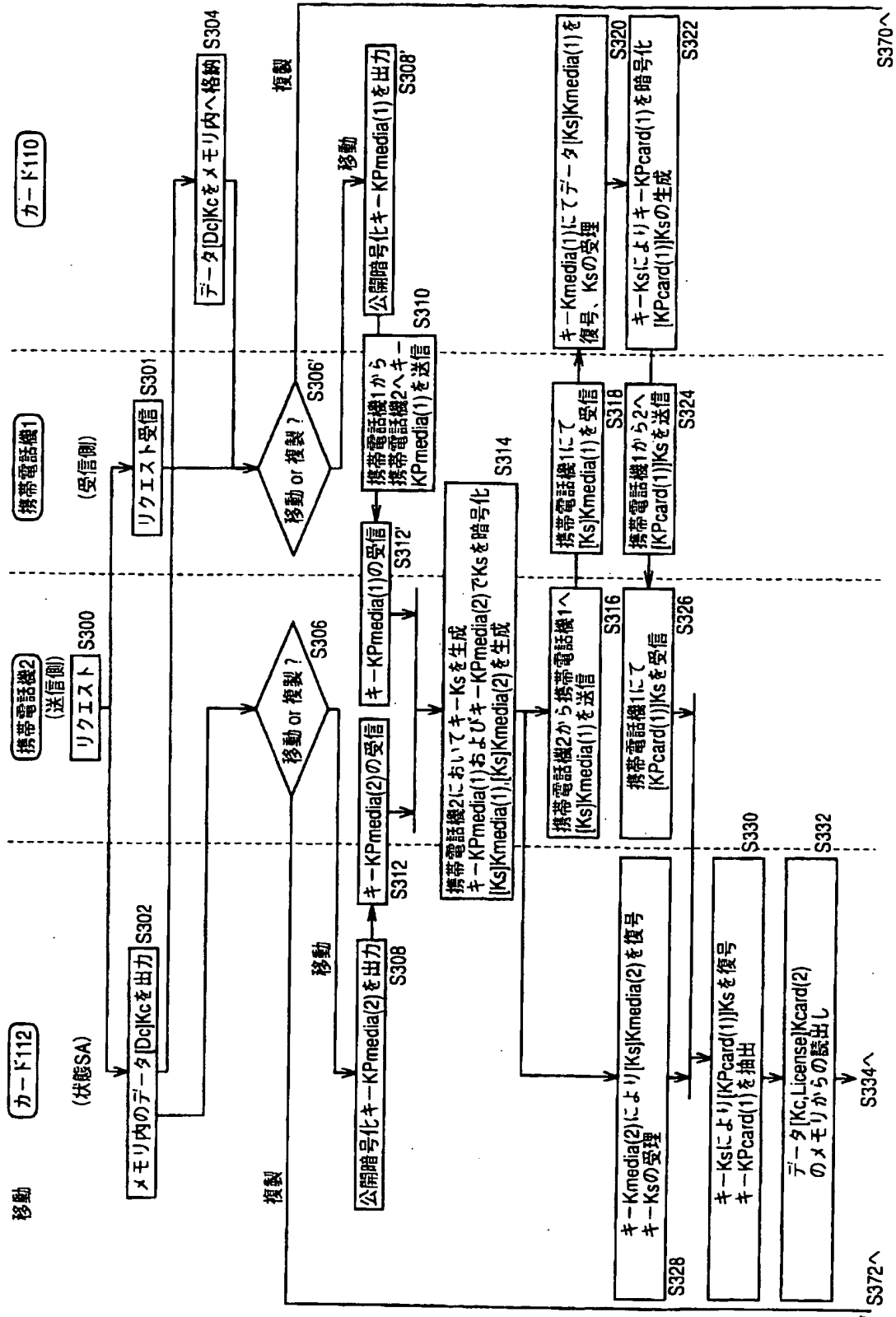


FIG.10

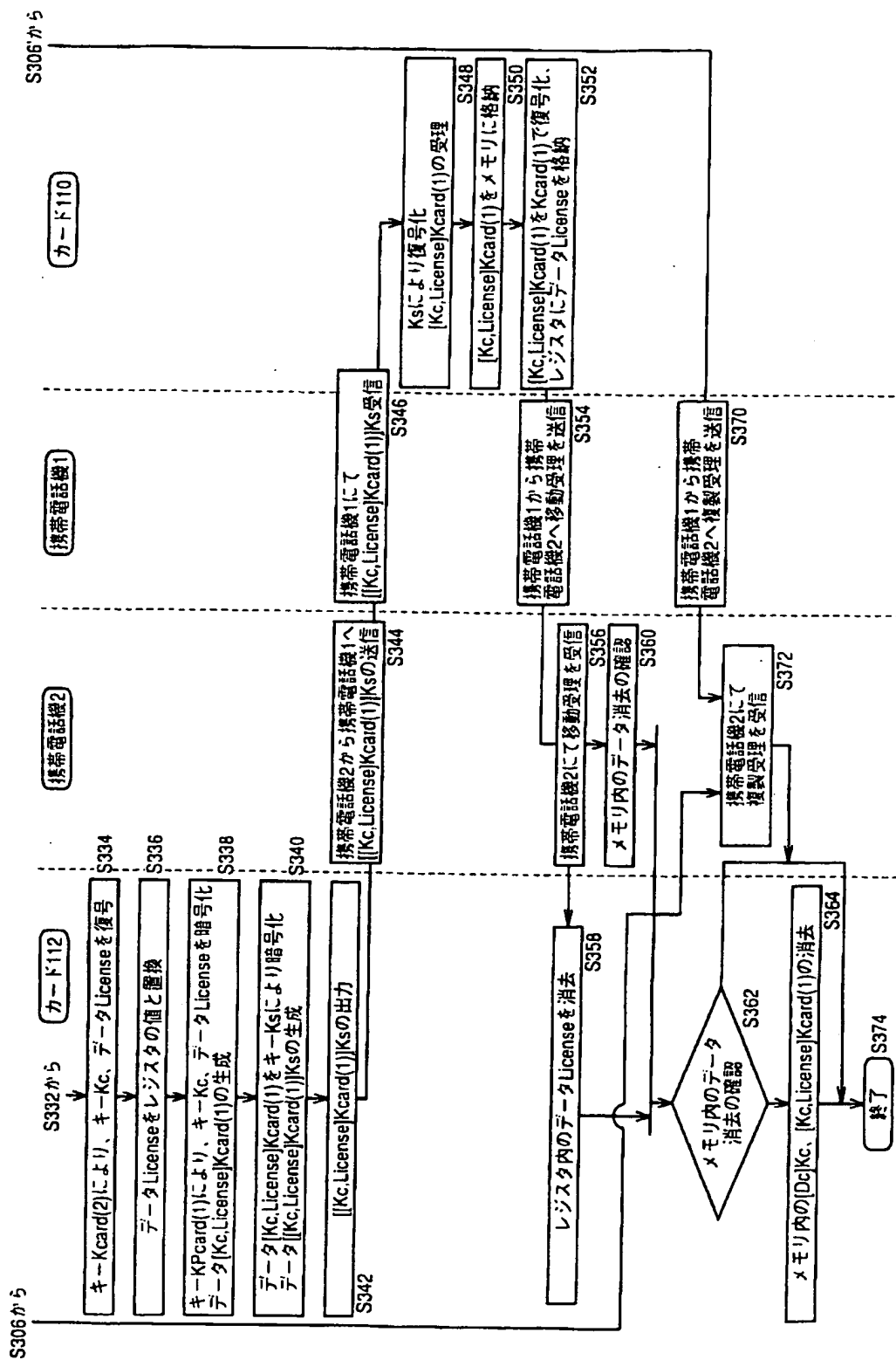


FIG.11

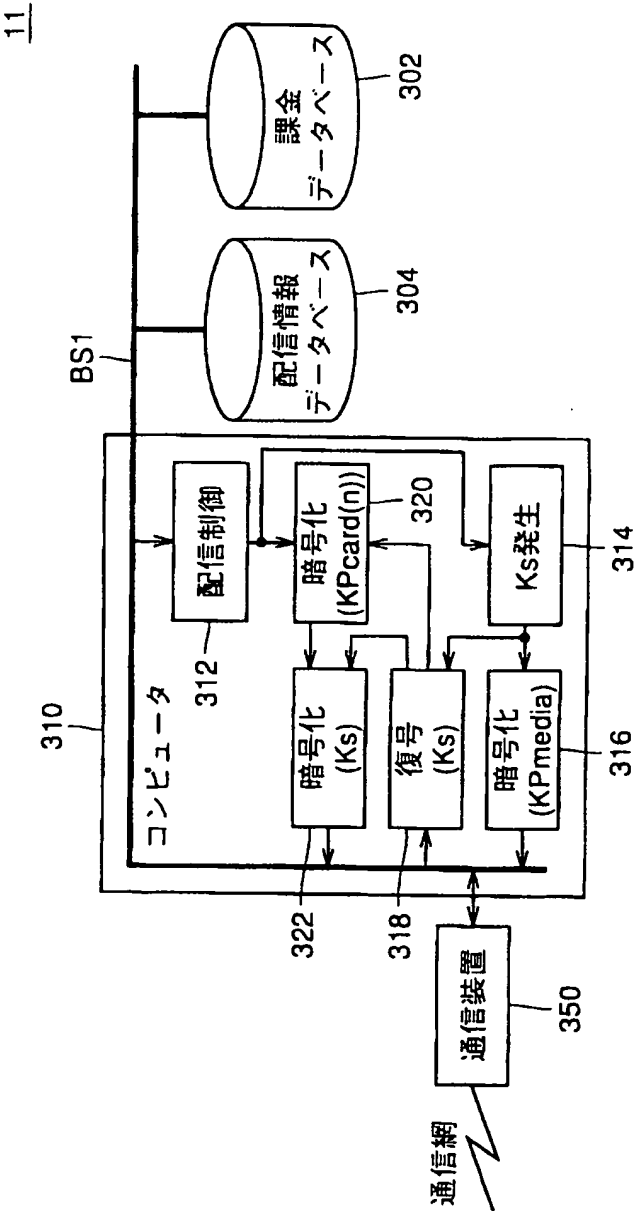
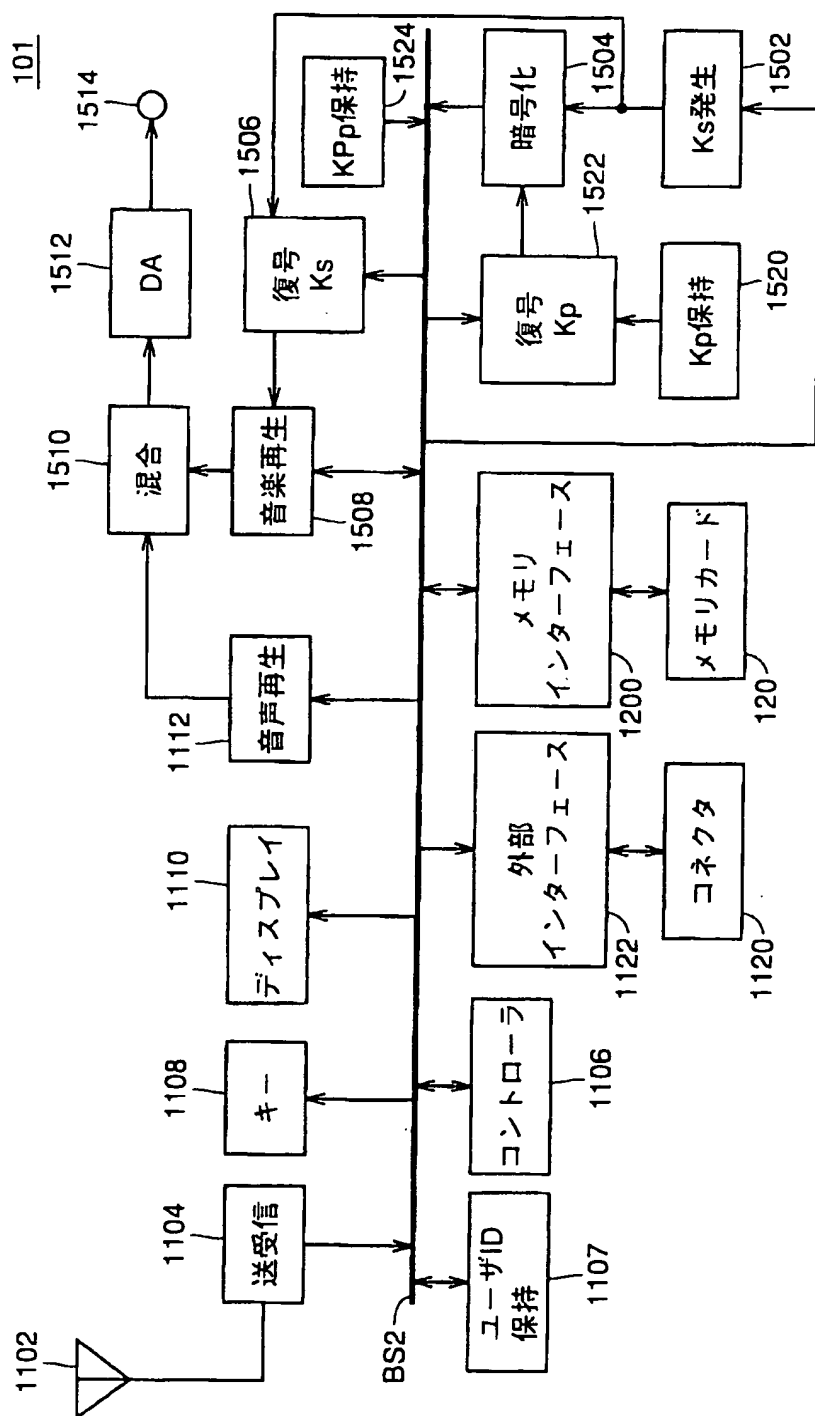


FIG. 12



**FIG. 13**

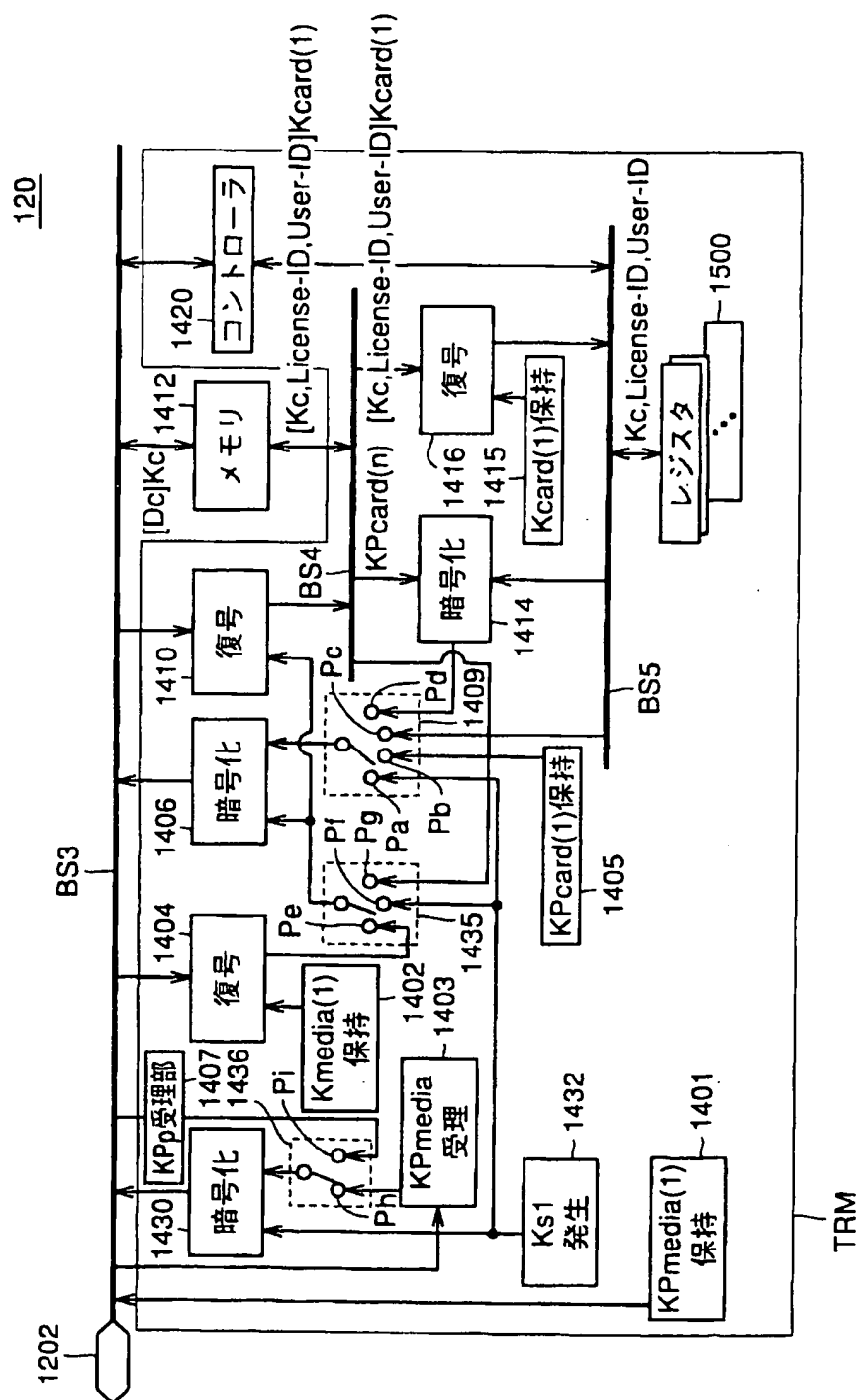


FIG. 14

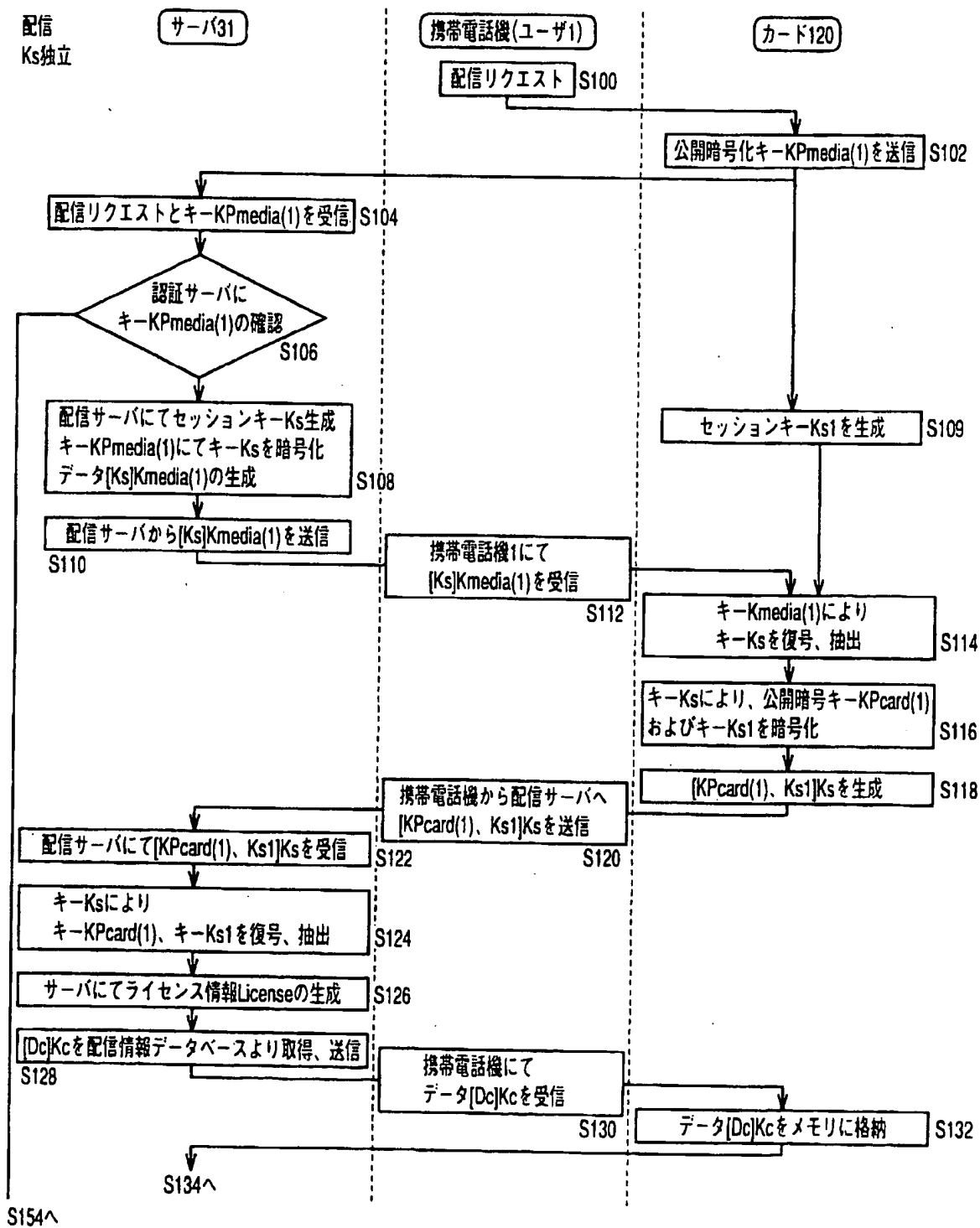


FIG. 15

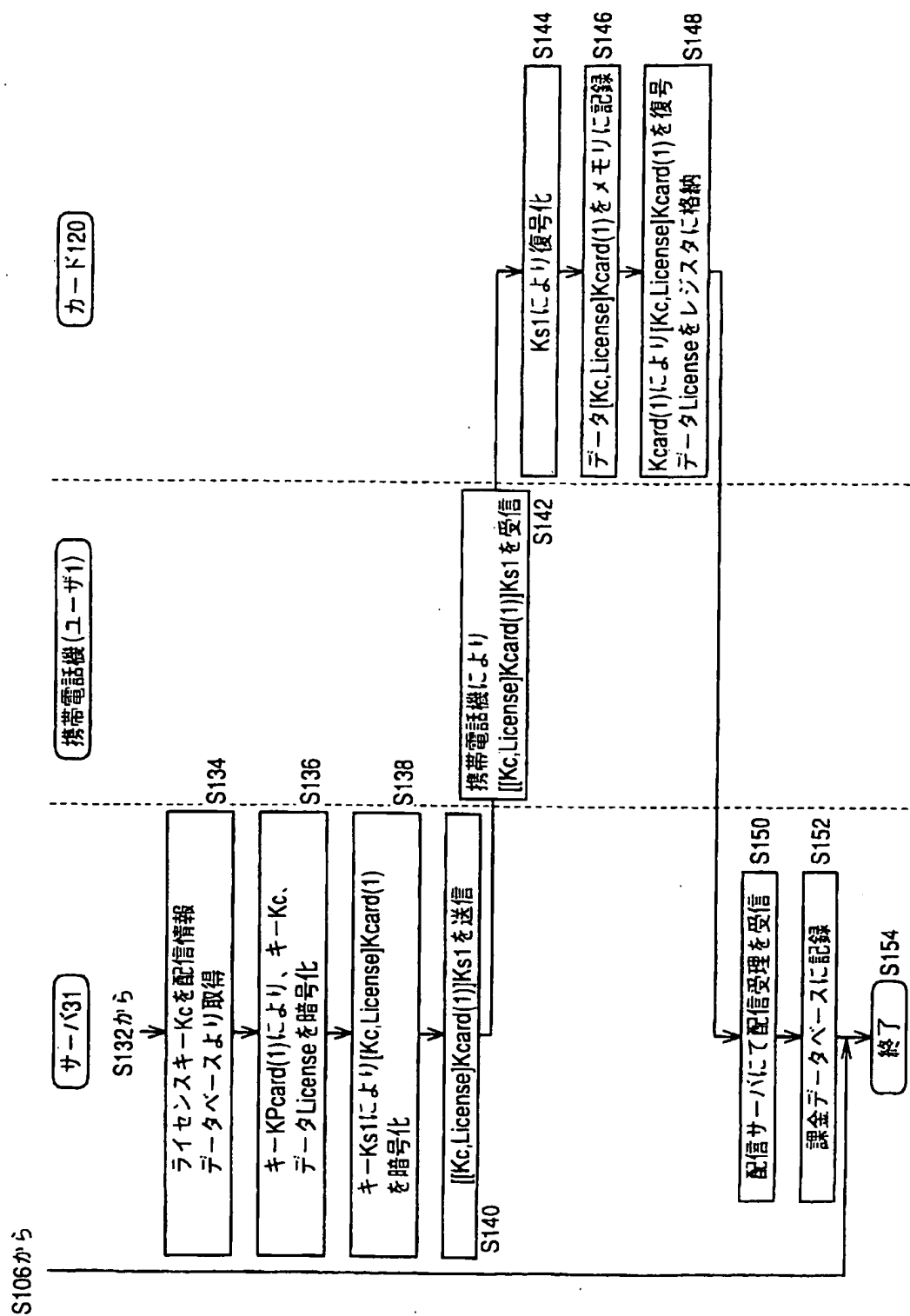




FIG. 16

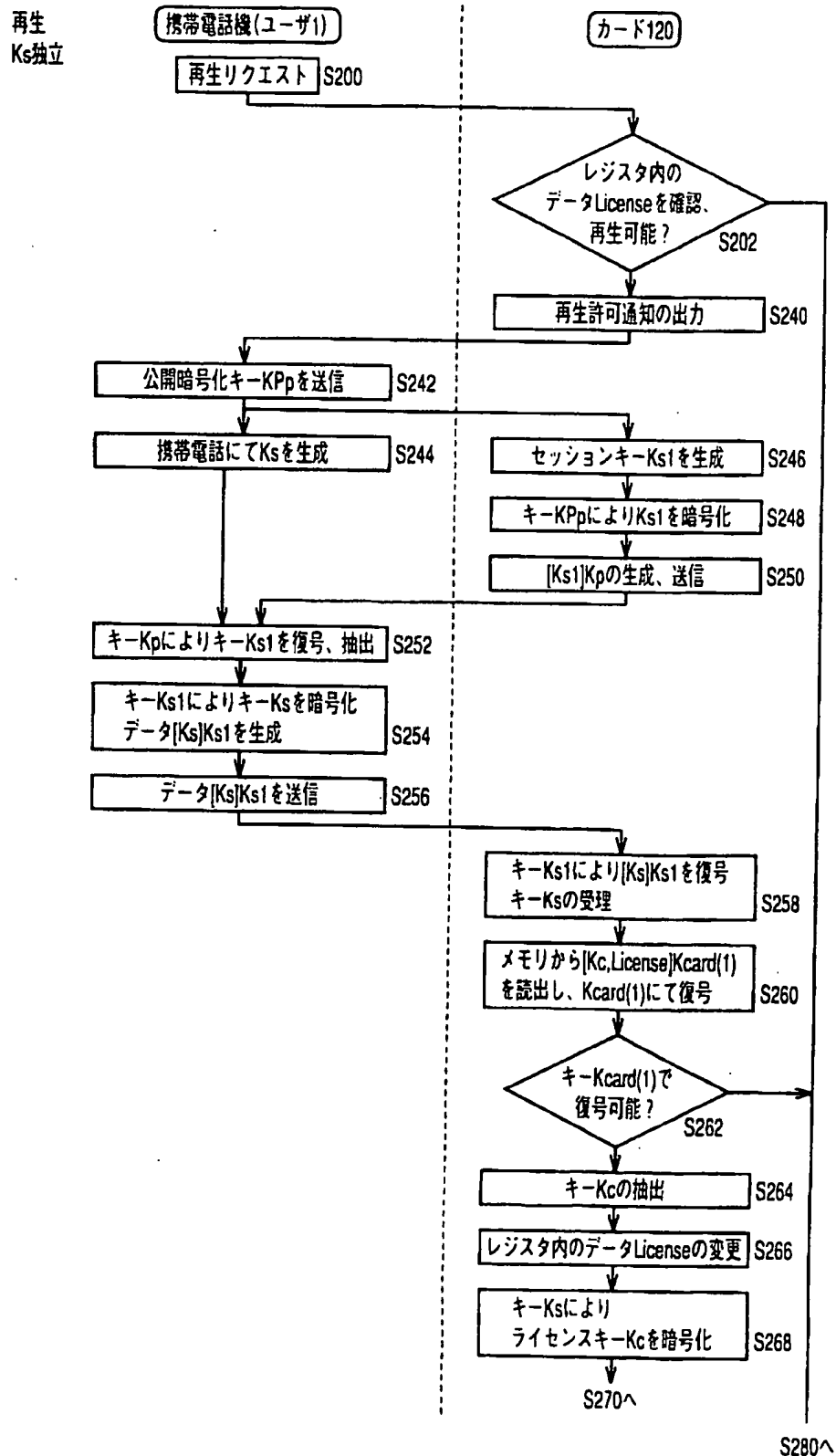


FIG. 17

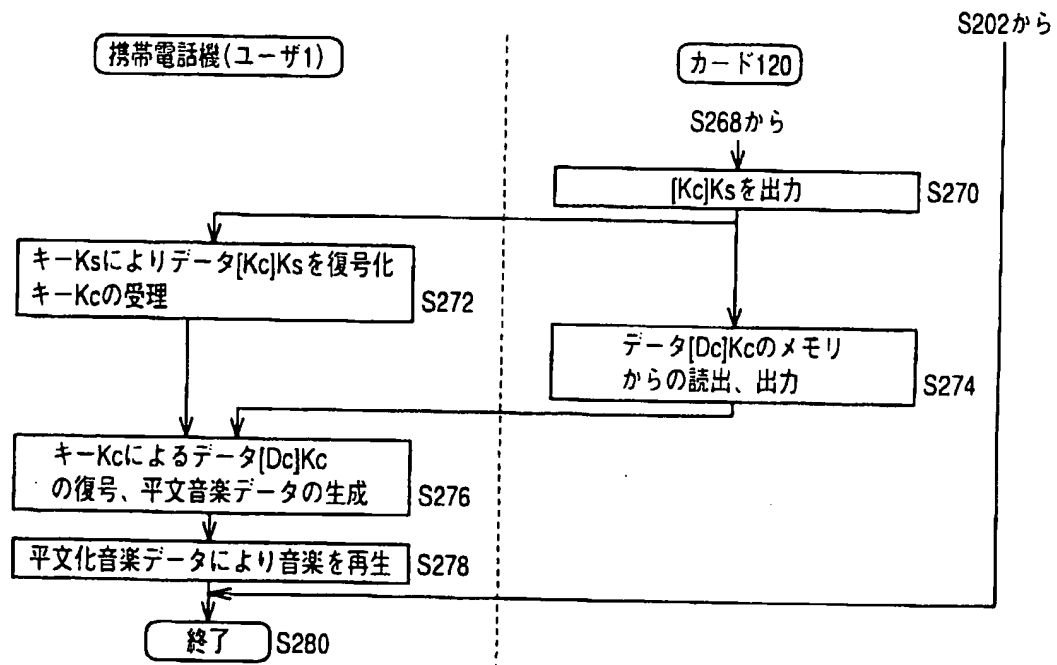


FIG.18

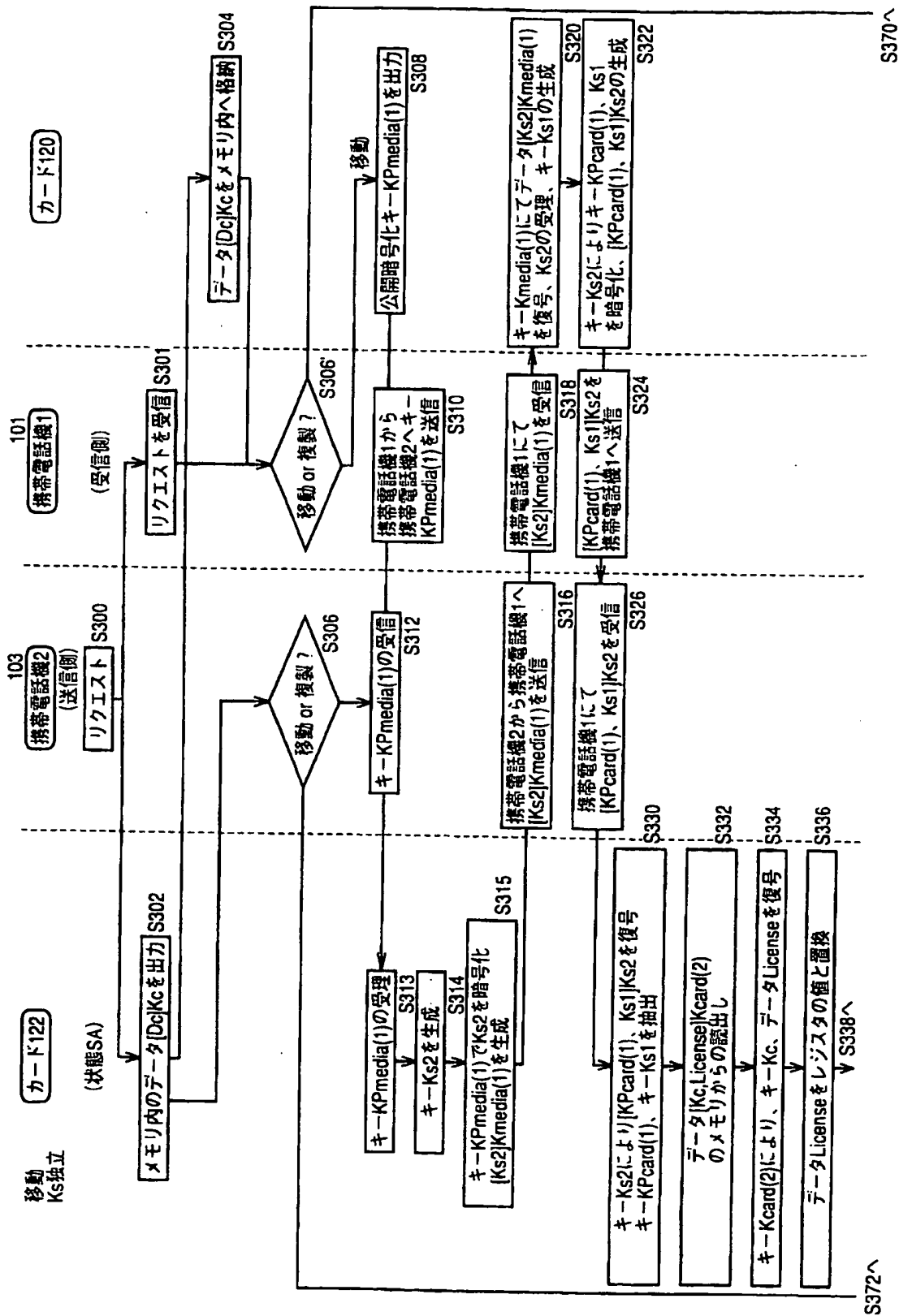


FIG.19

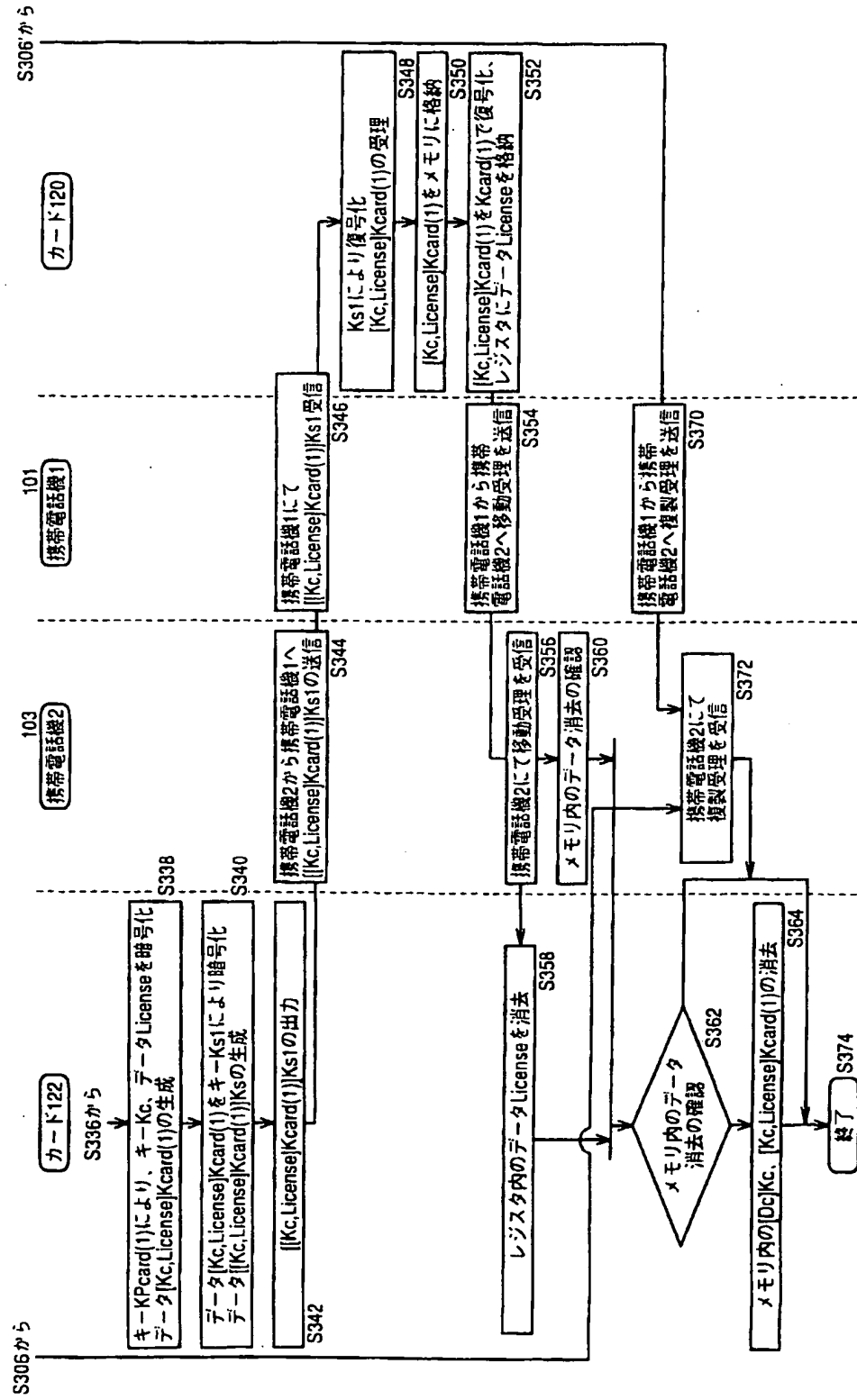


FIG.20

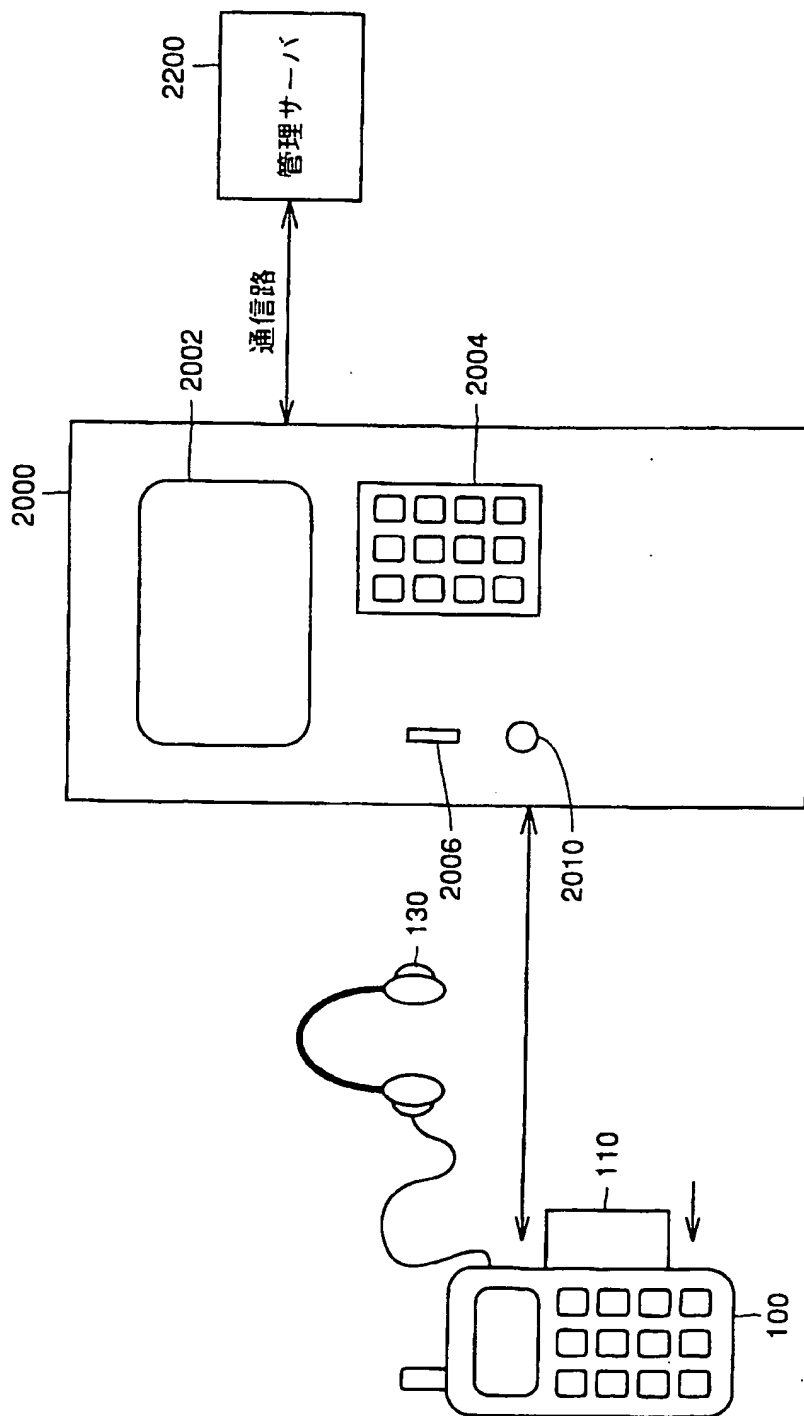


FIG.21

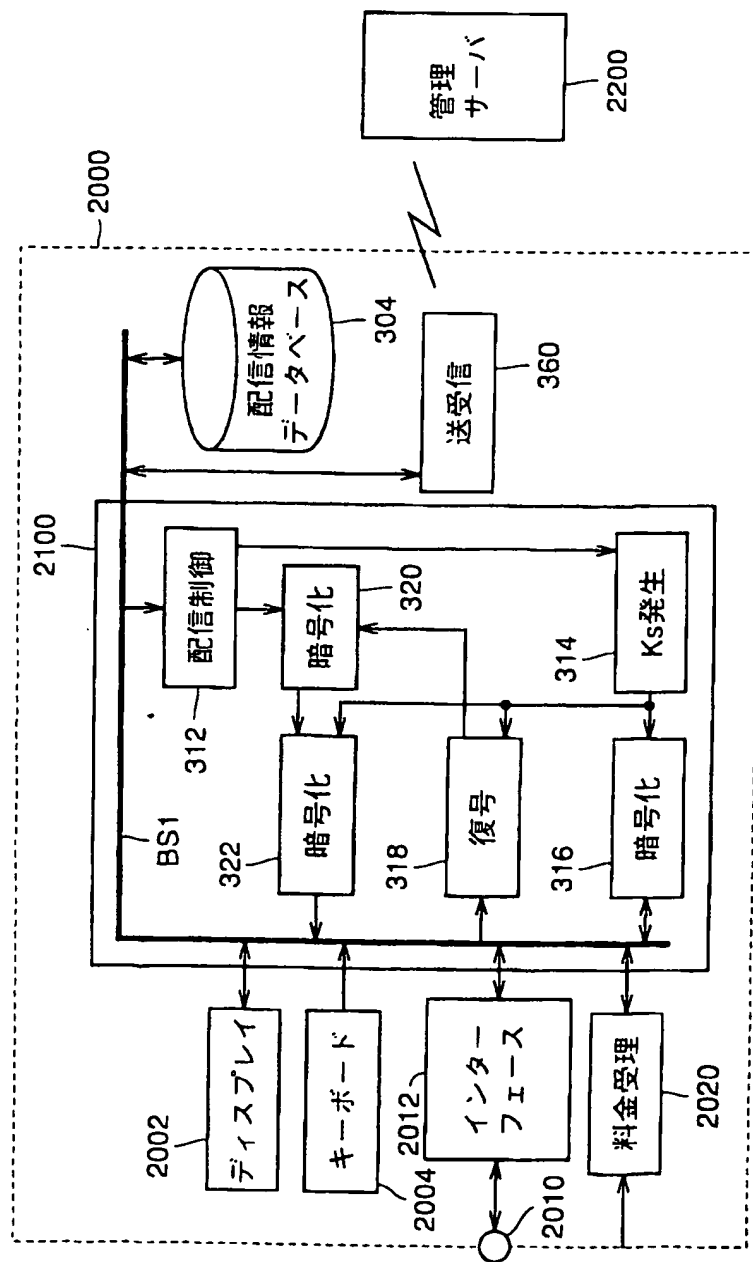


FIG.22

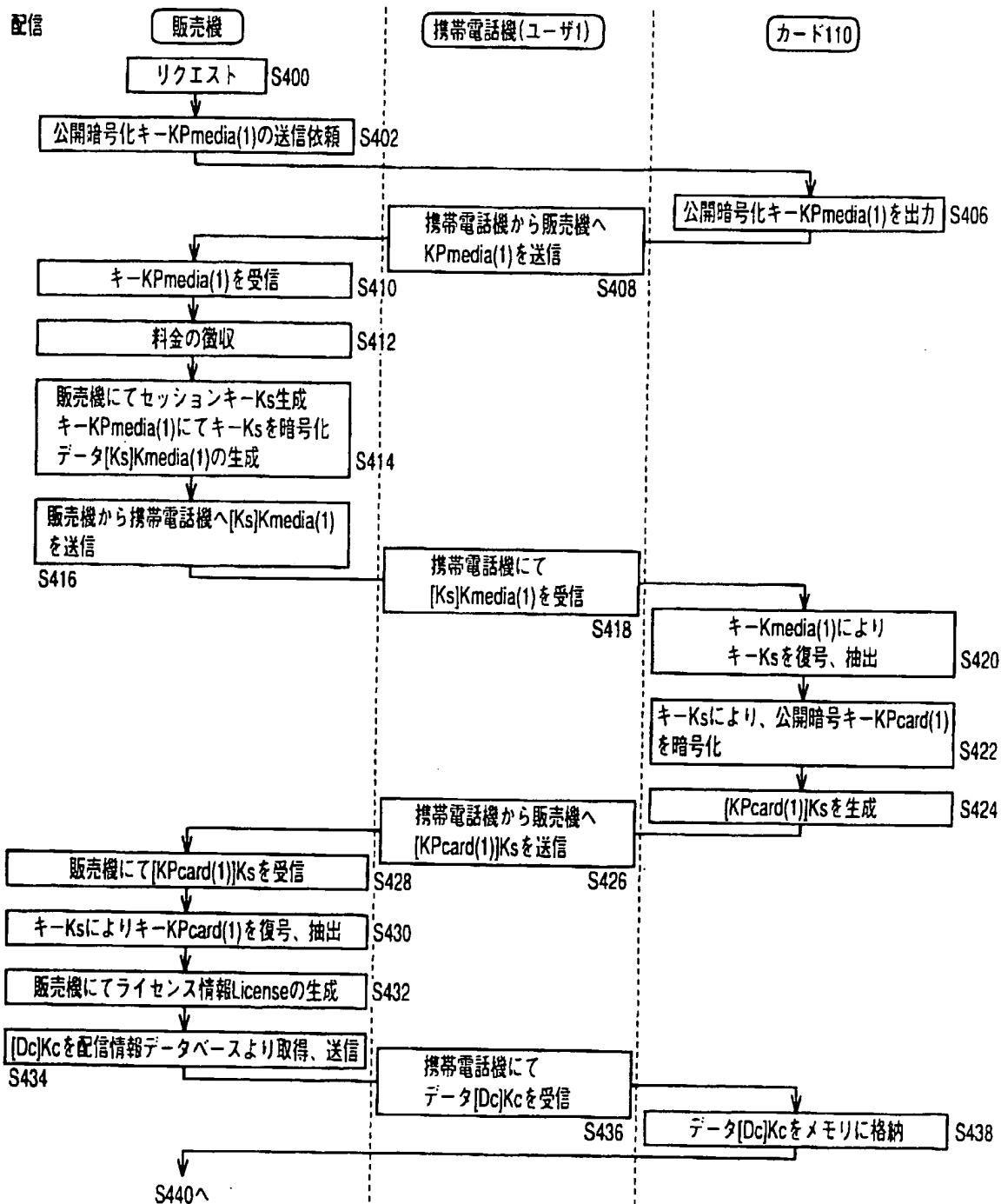
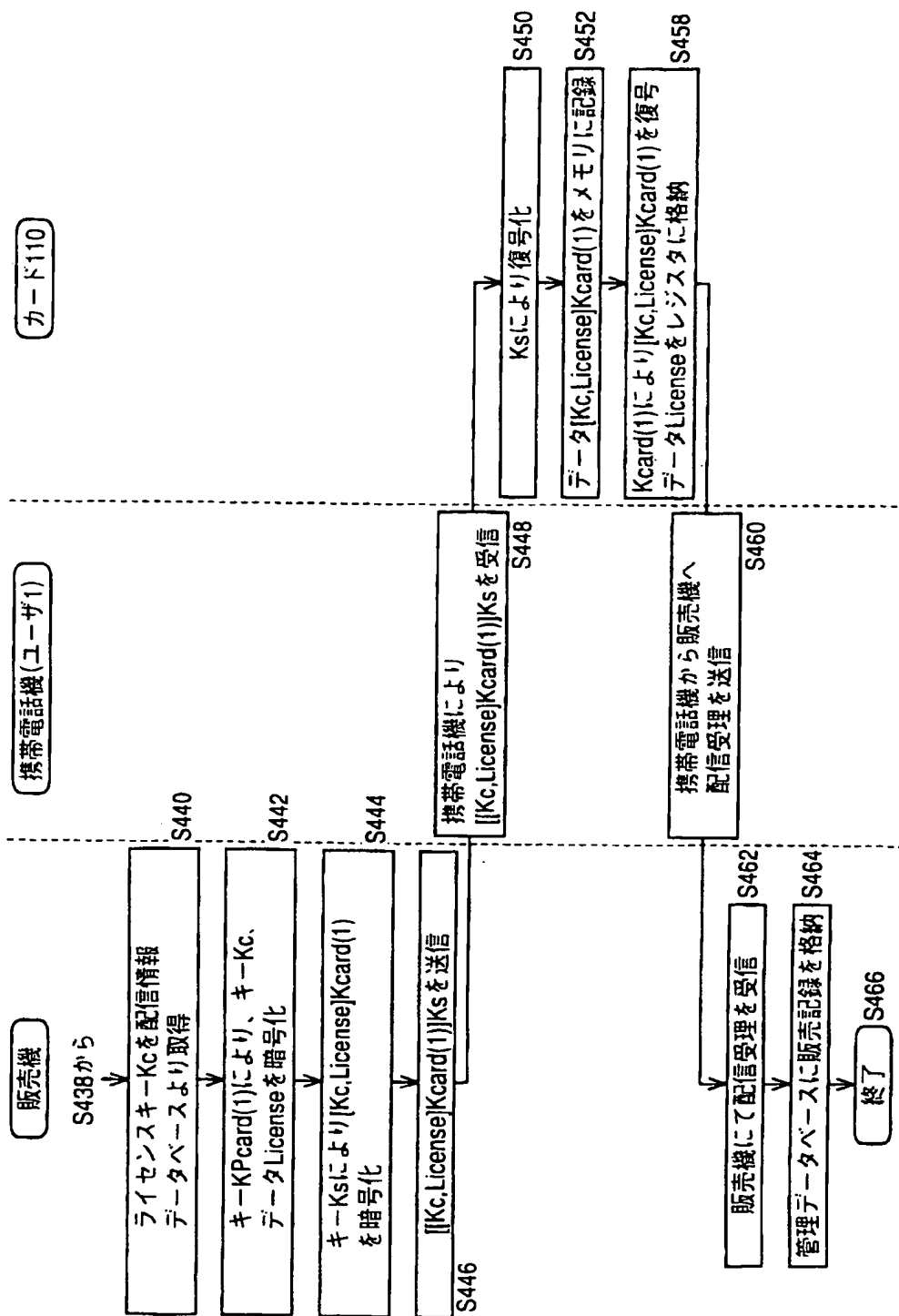


FIG.23





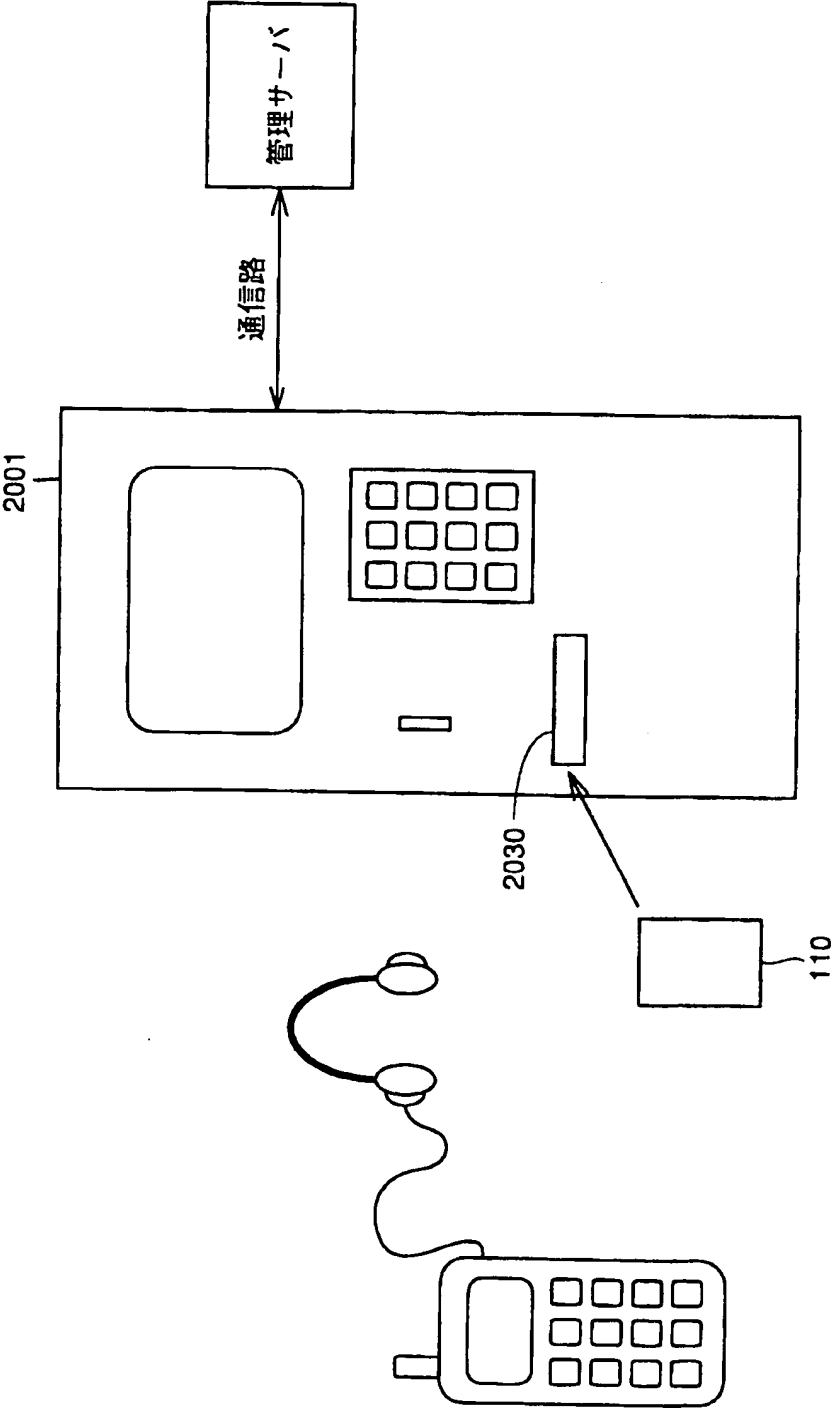


FIG.24

FIG.25

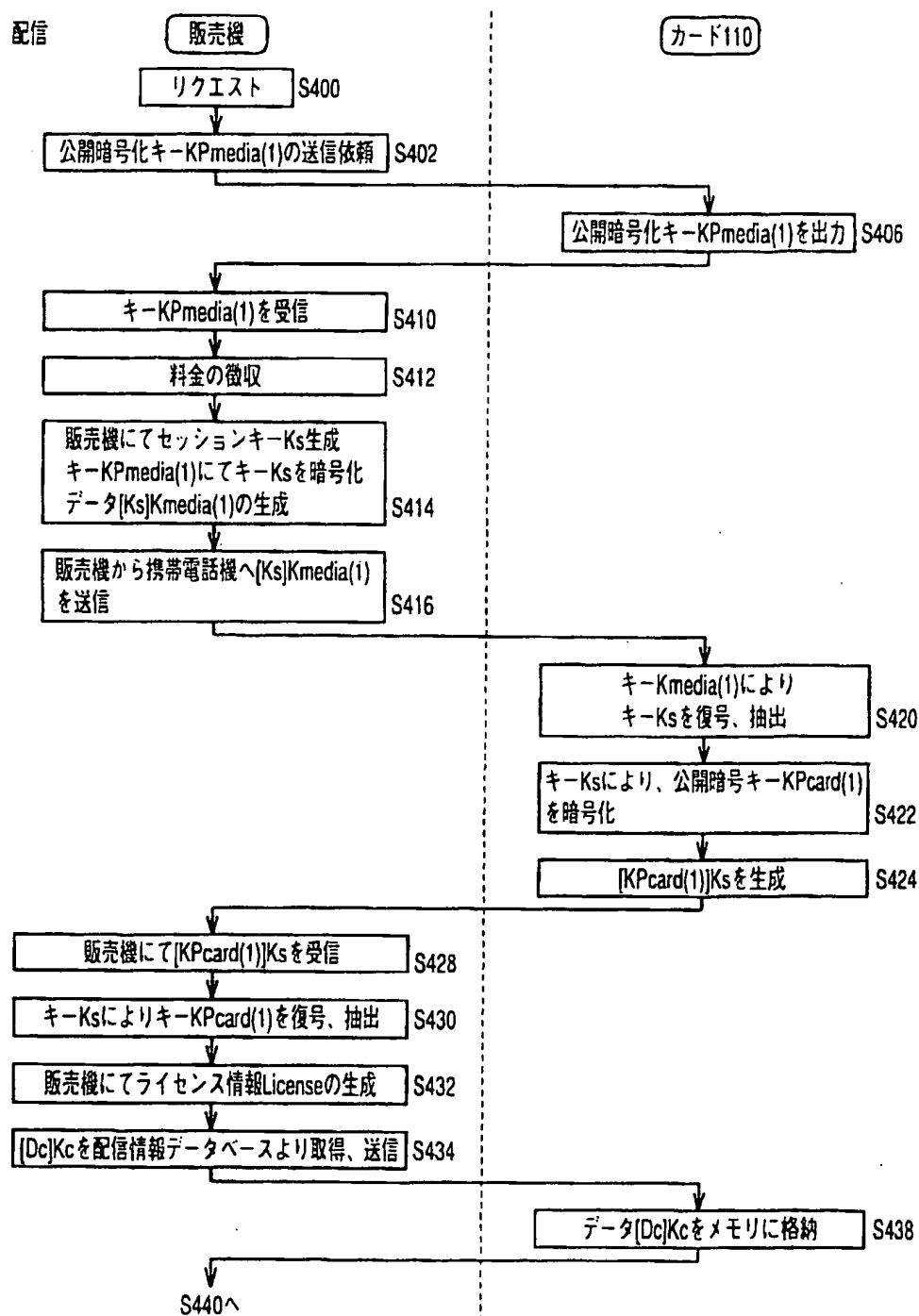


FIG.26

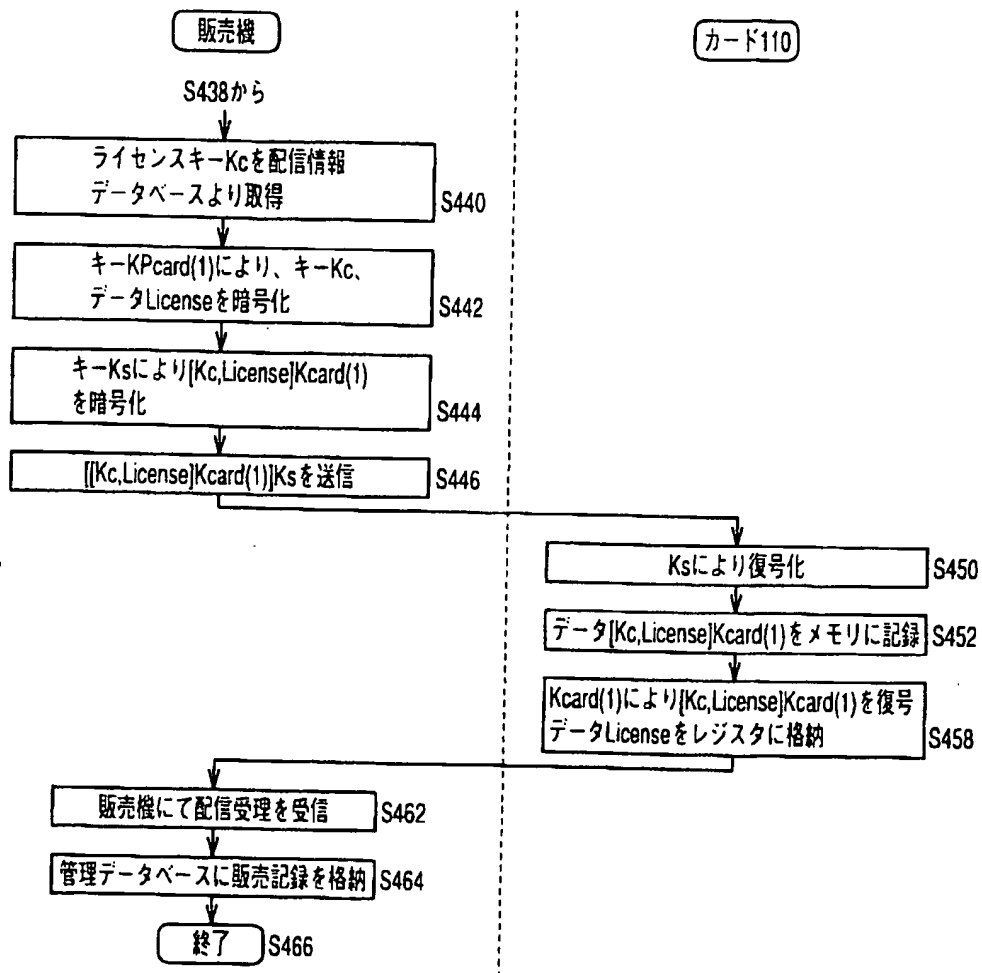


FIG.27

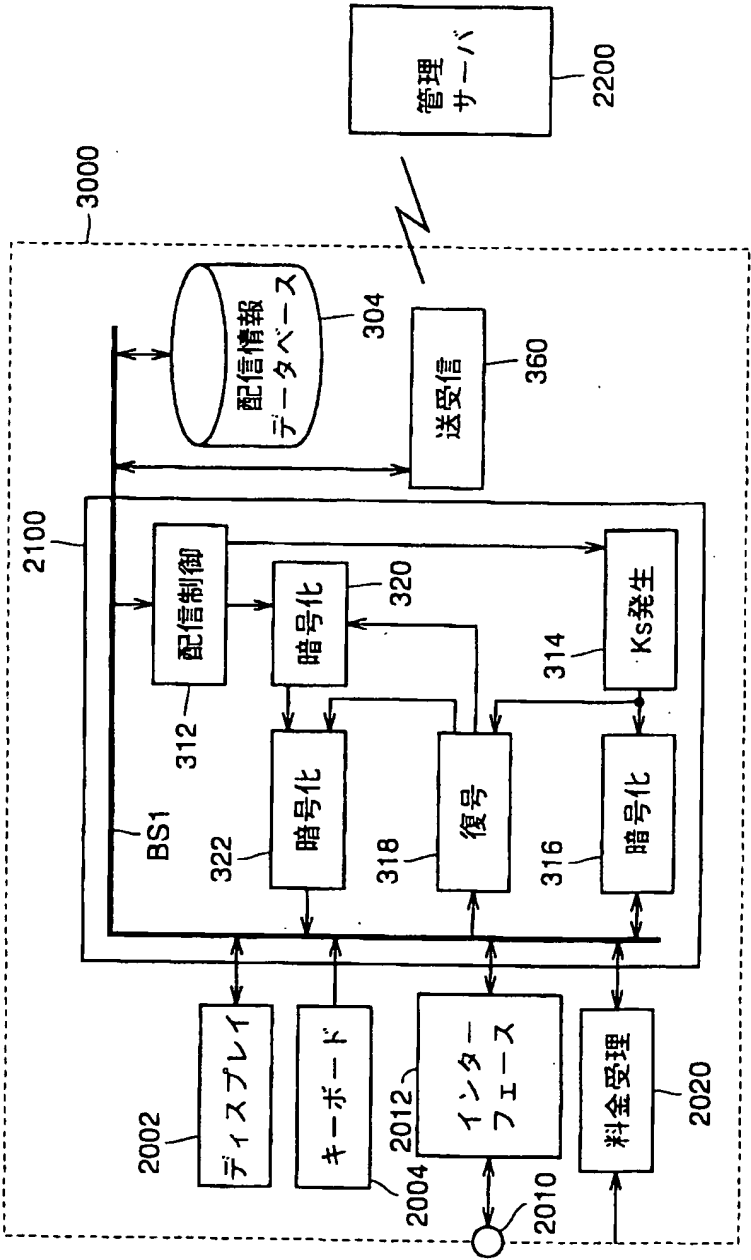


FIG. 28

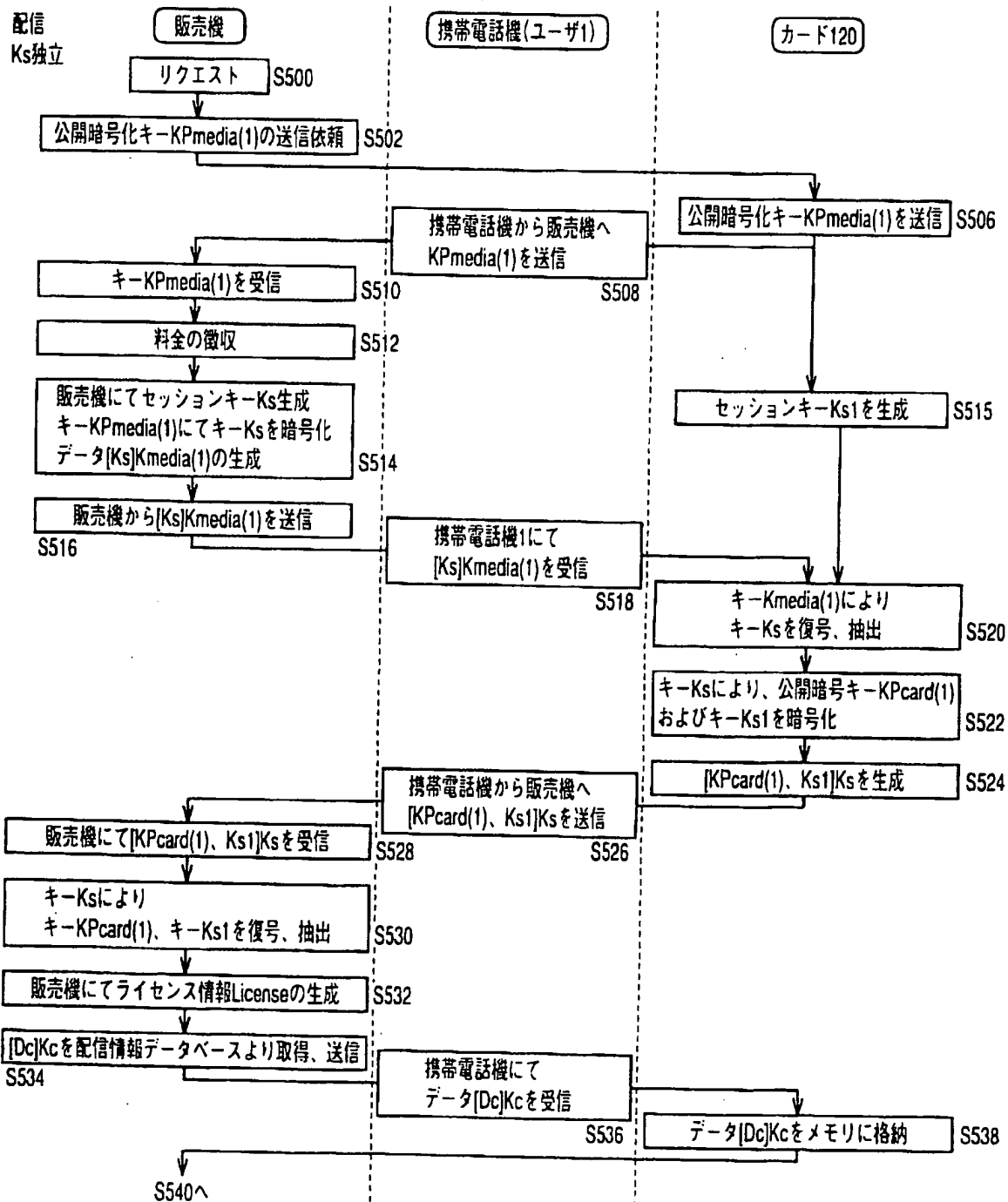


FIG.29

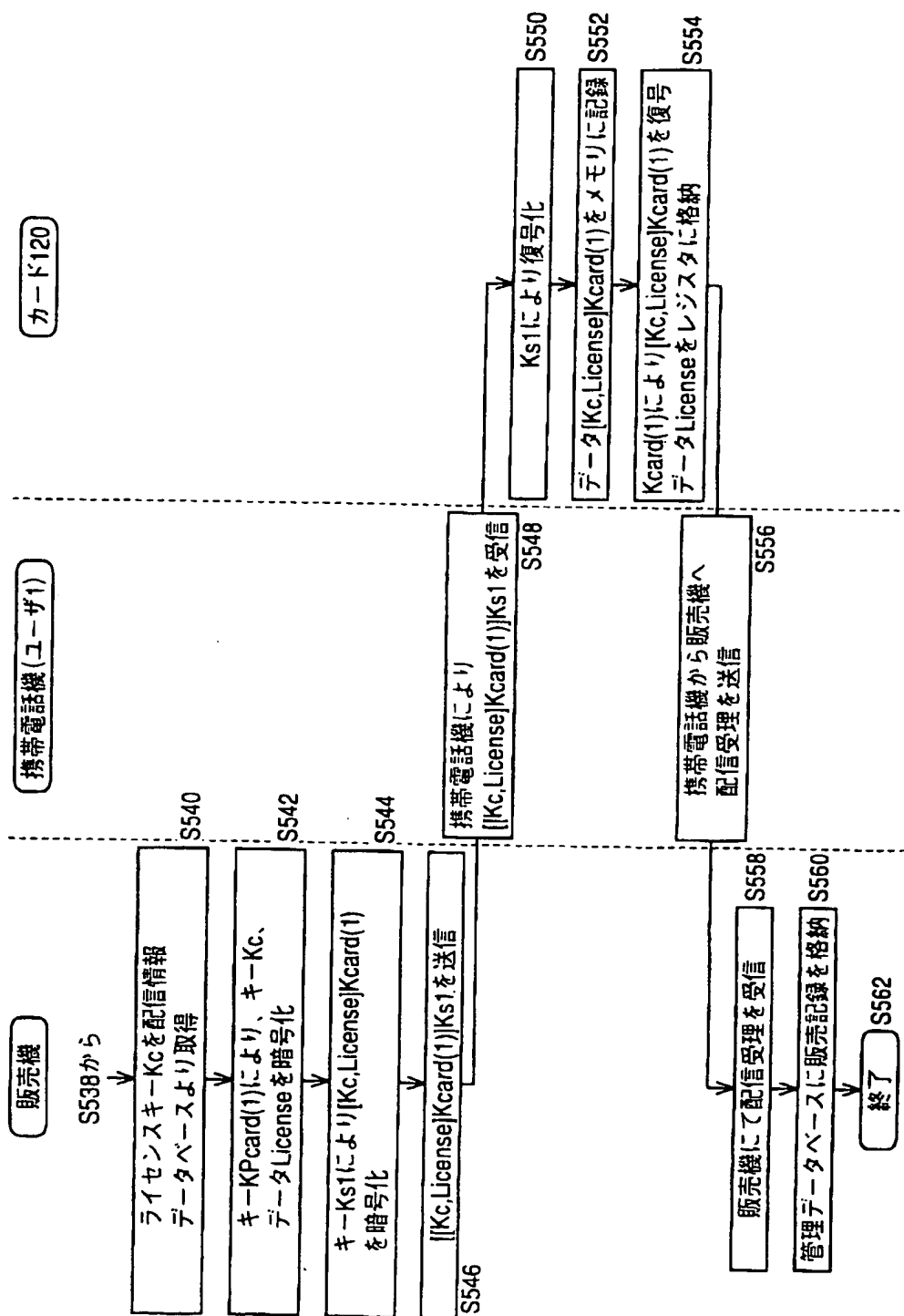


FIG.30

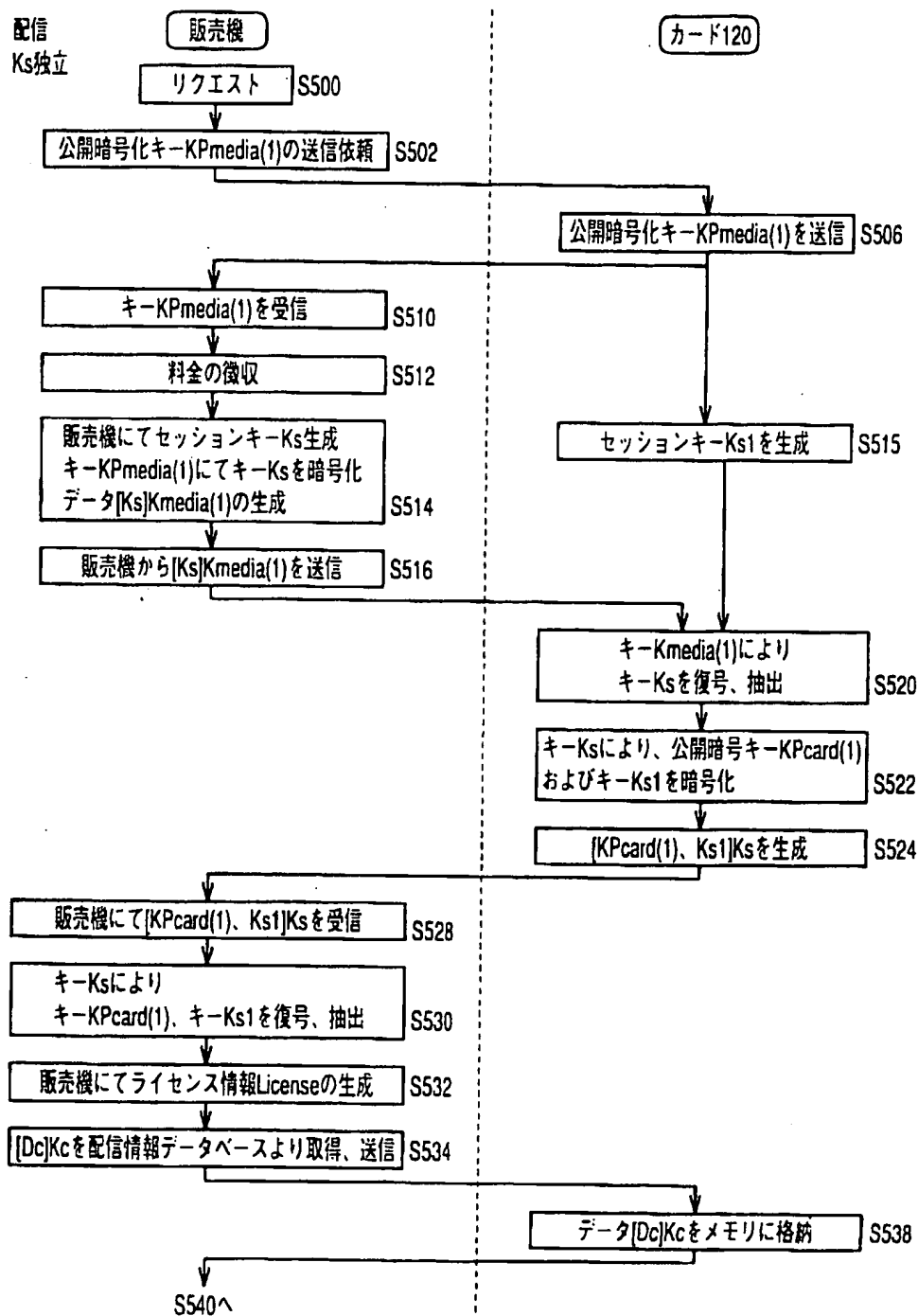


FIG.31

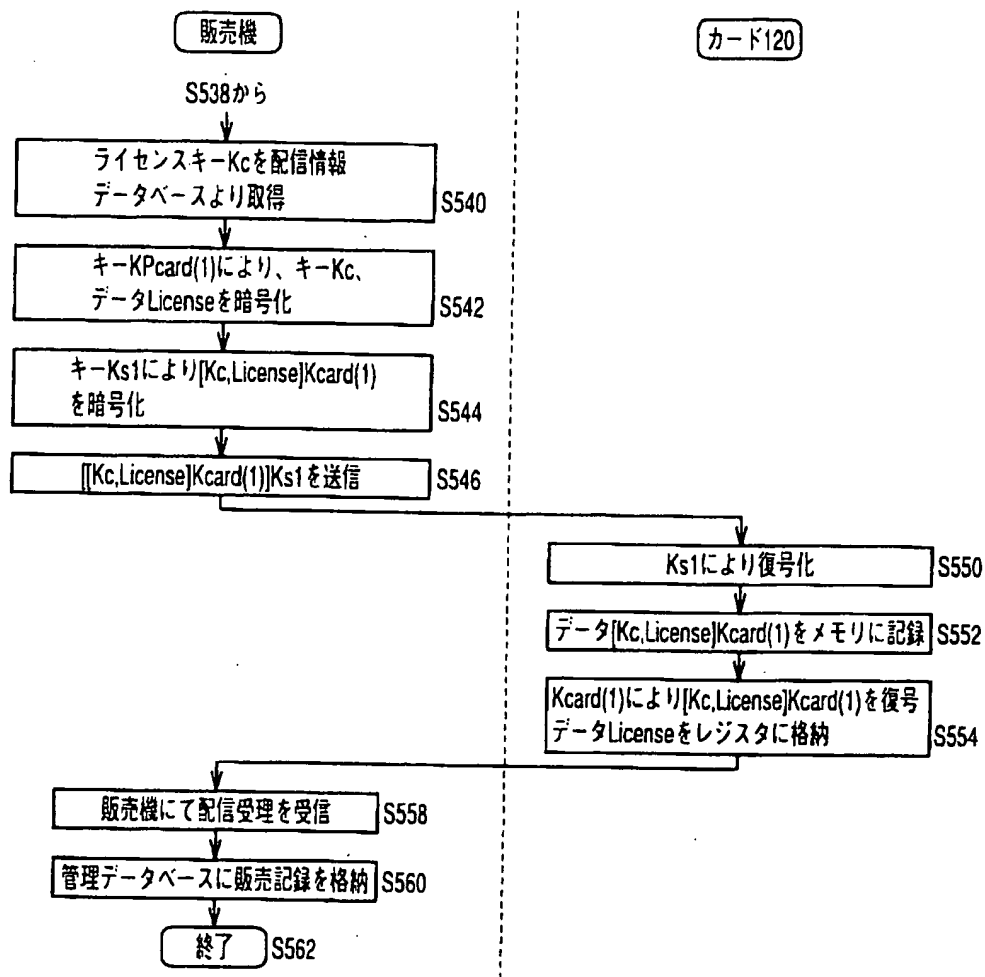




FIG.32

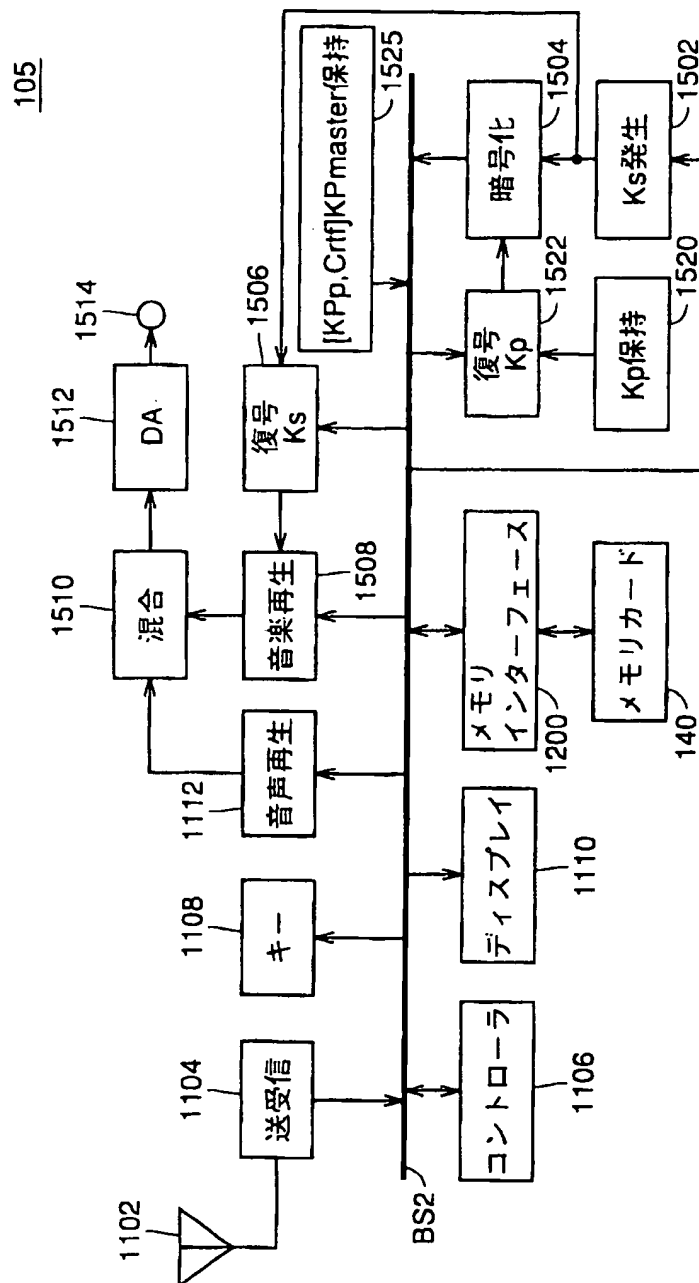


FIG.33

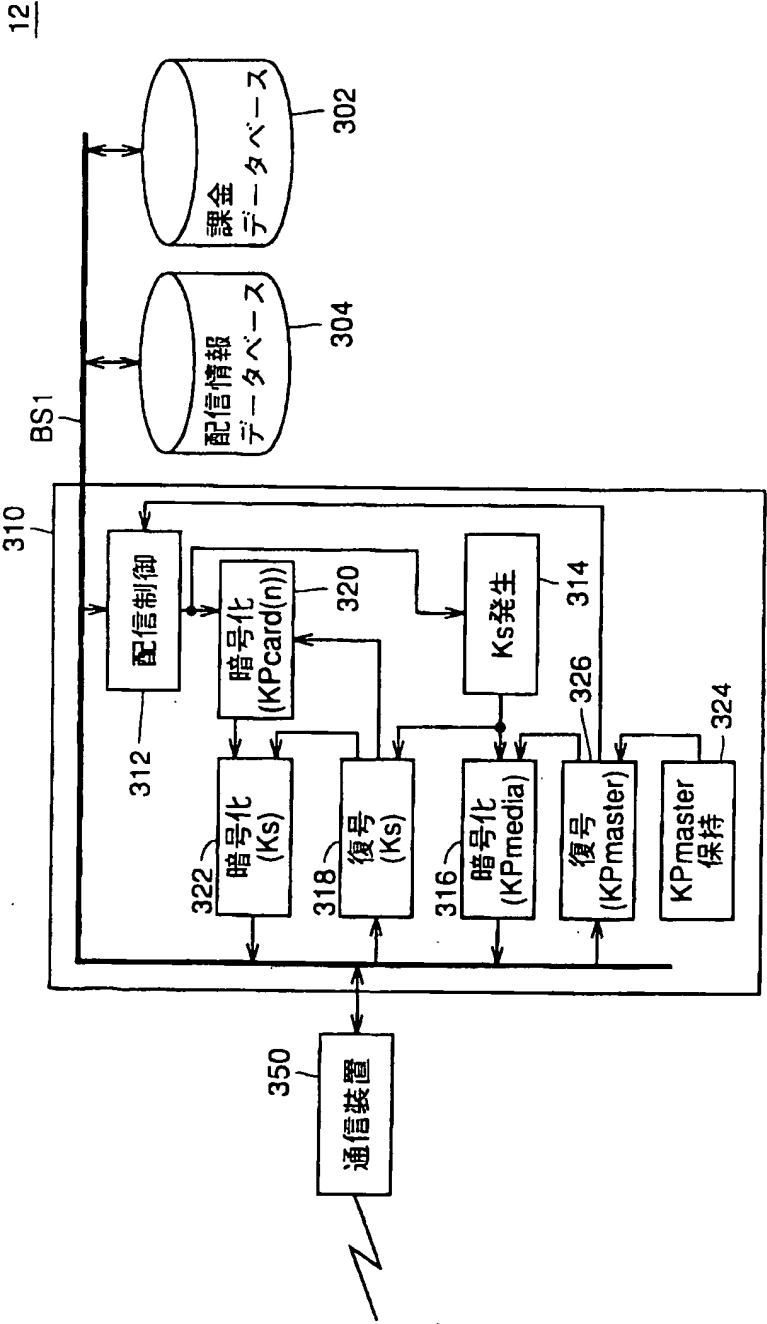


FIG.34

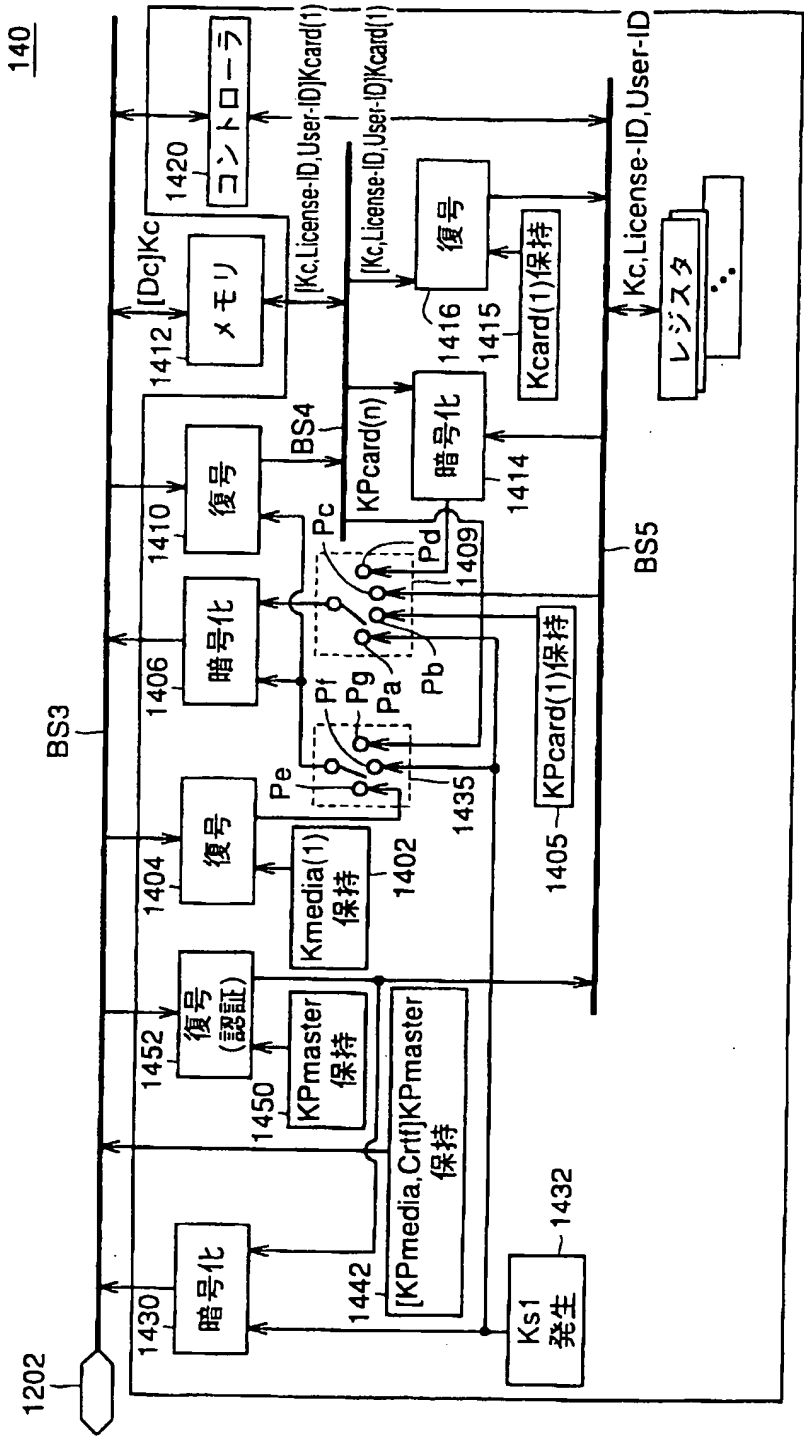


FIG. 35

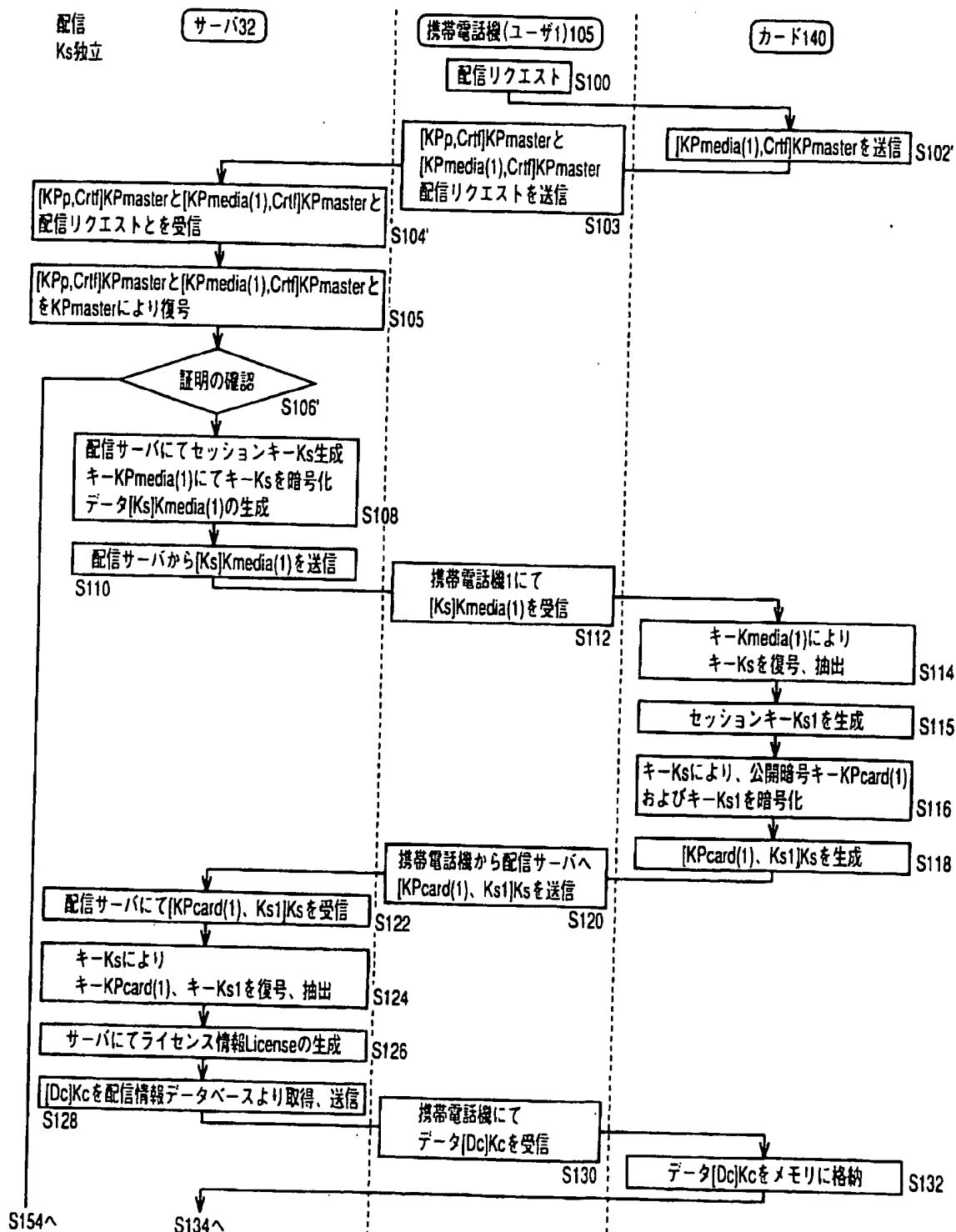


FIG.36

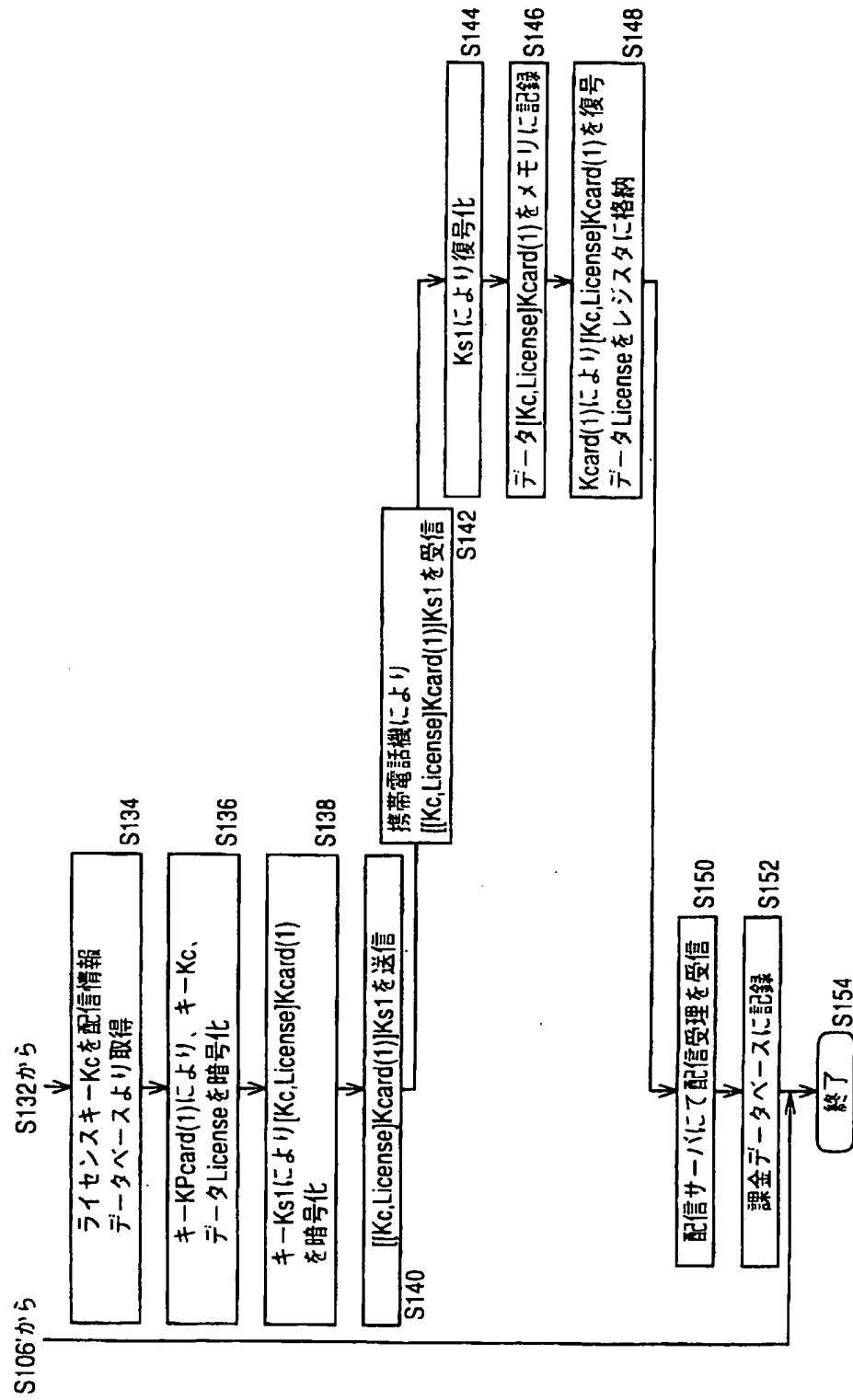


FIG. 37

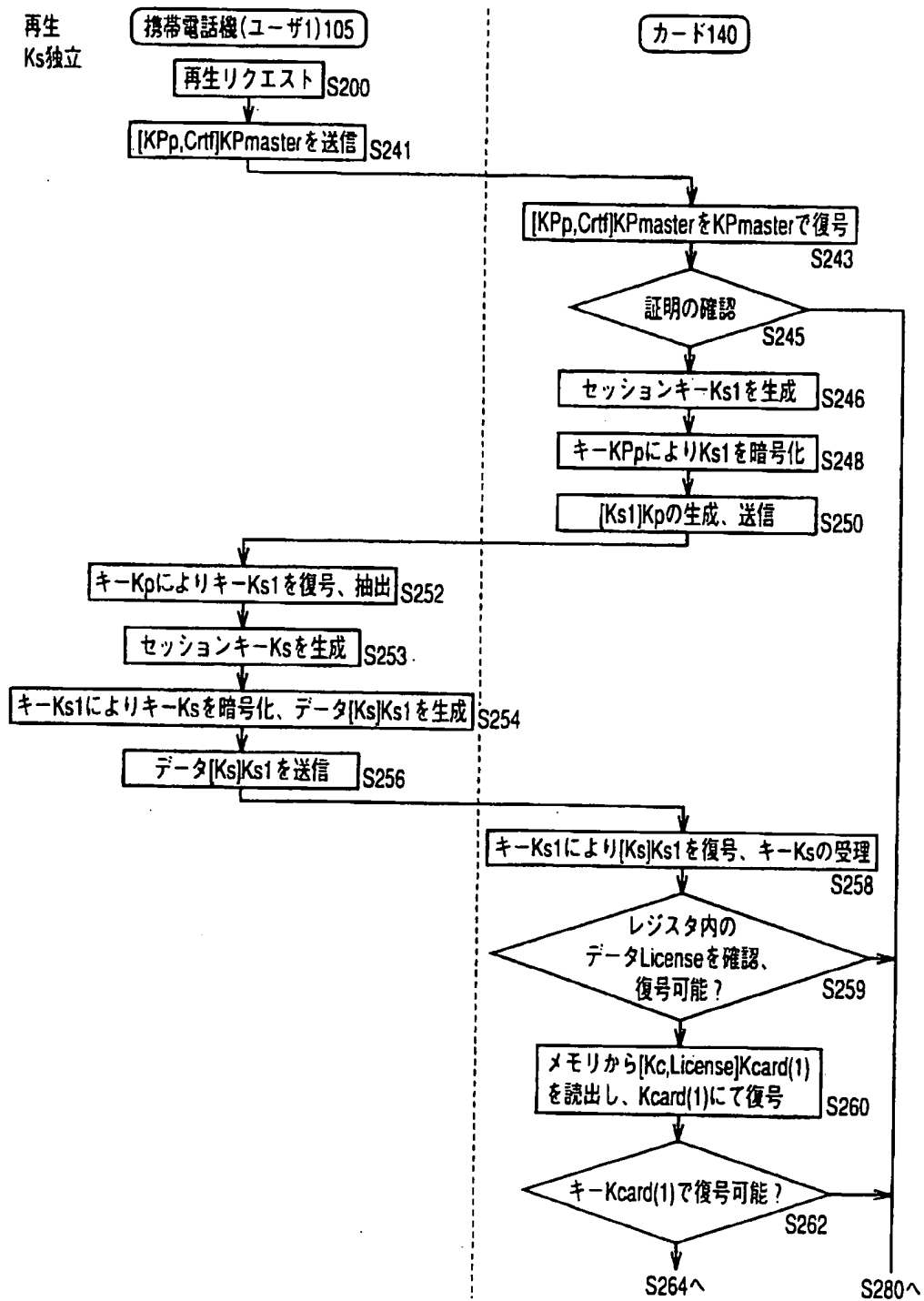
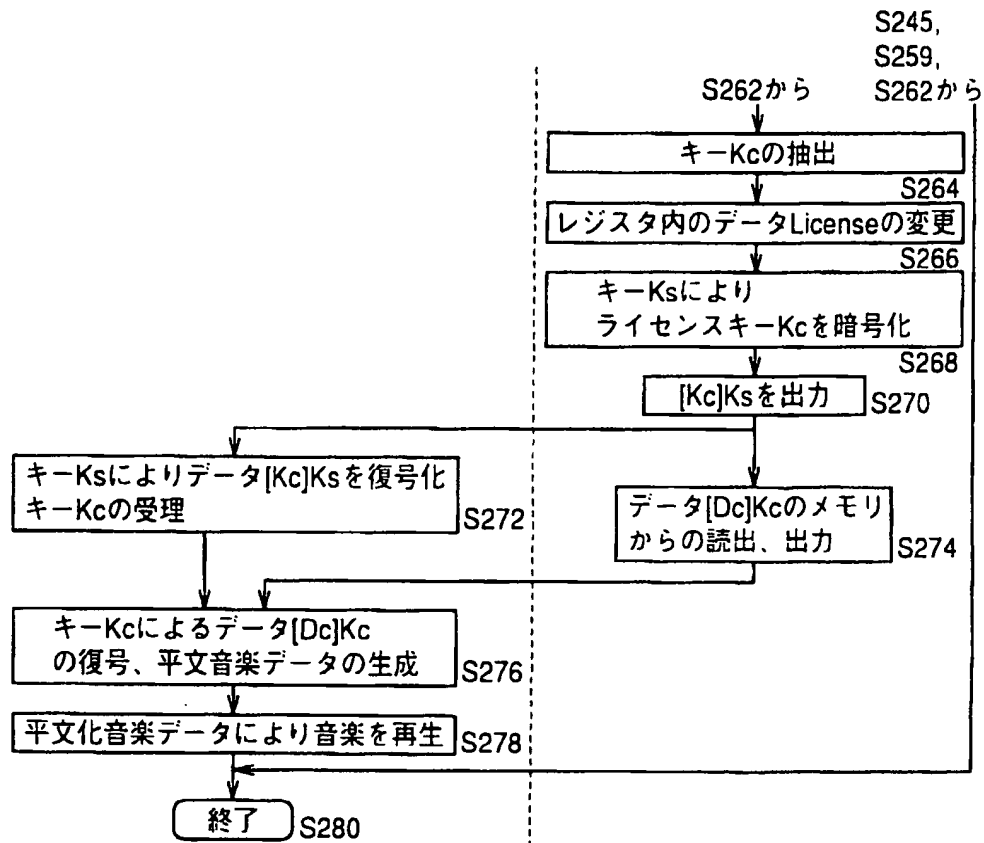


FIG.38



**FIG. 39**

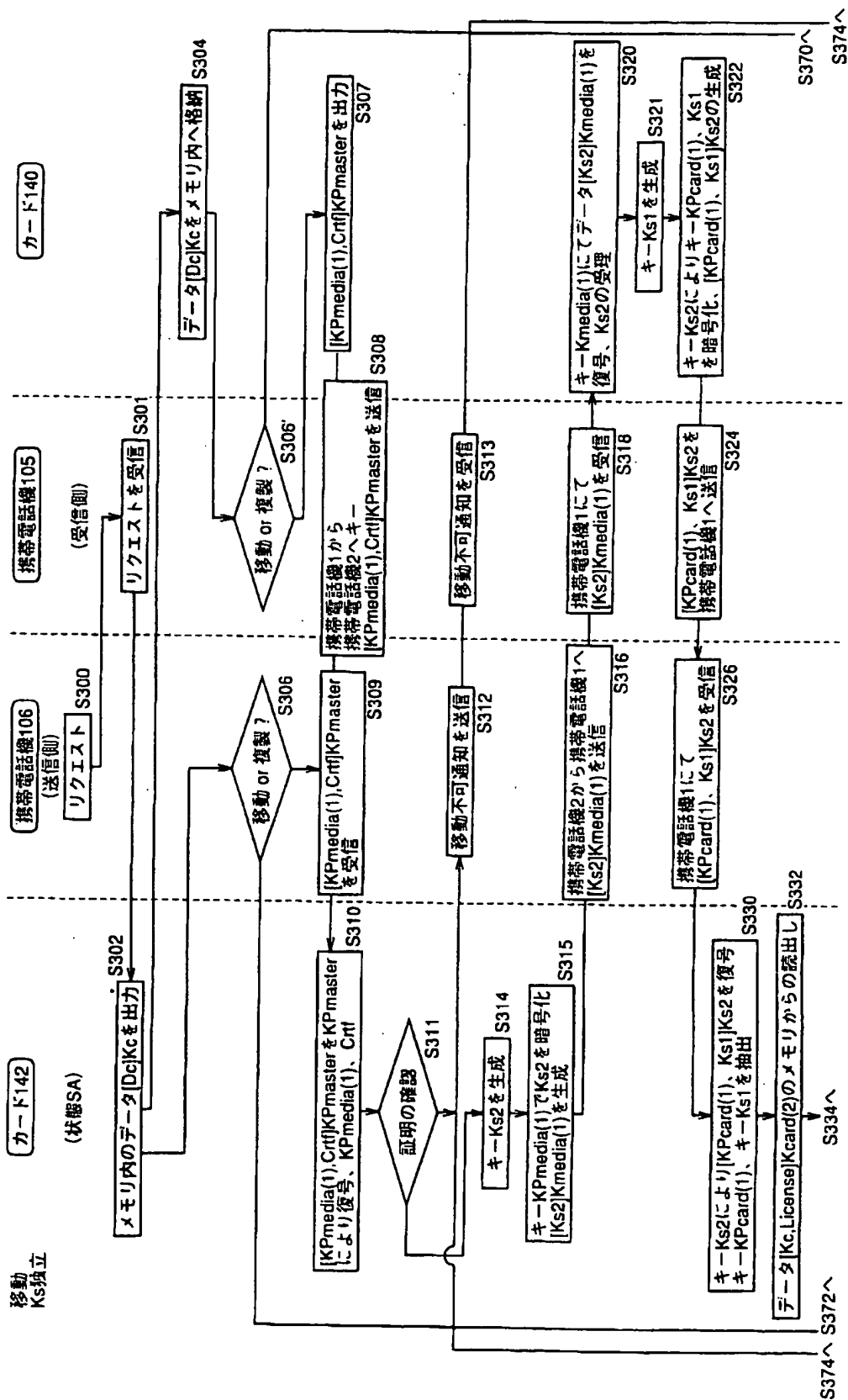




FIG. 40

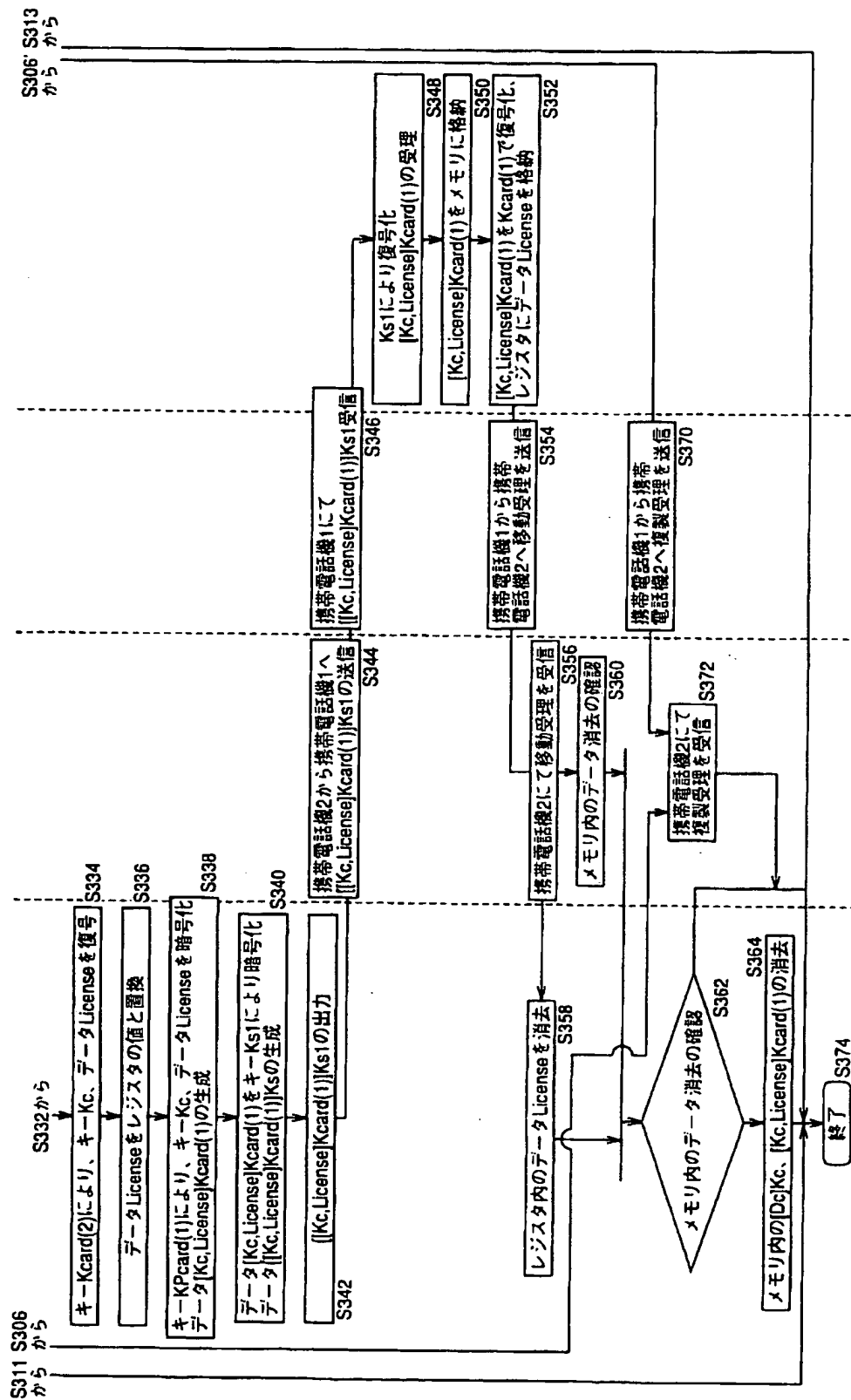


FIG.41

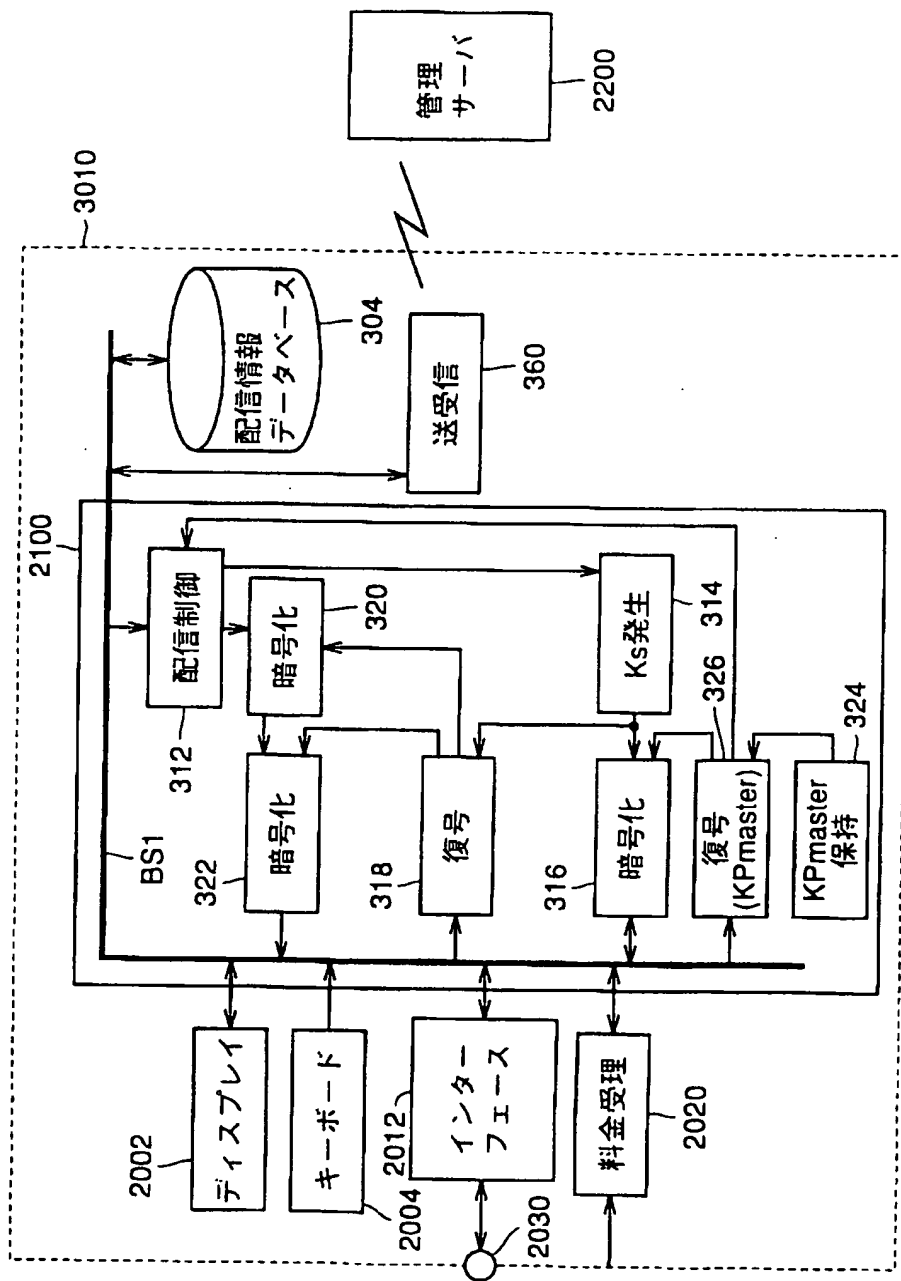


FIG. 42

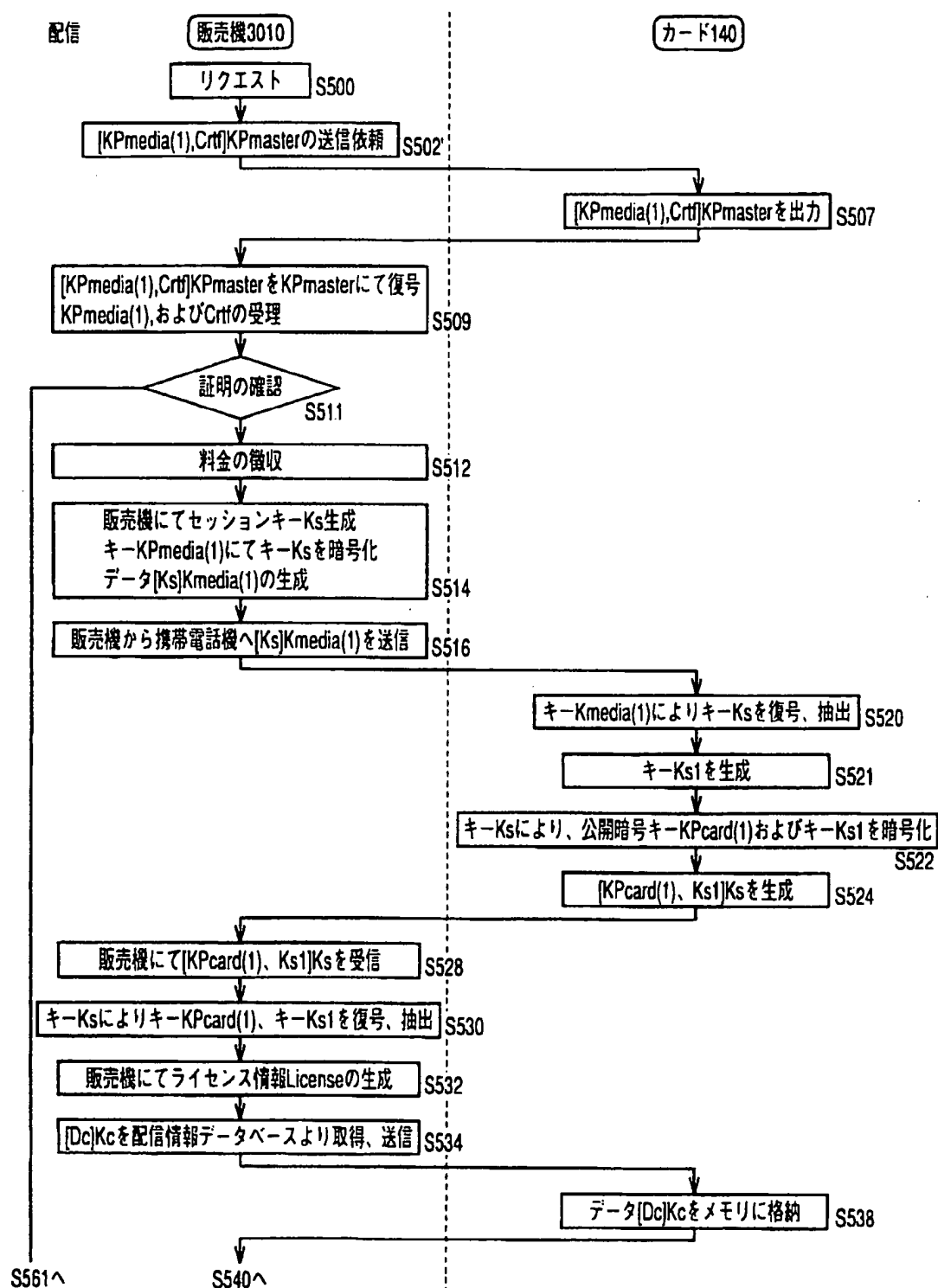


FIG. 43

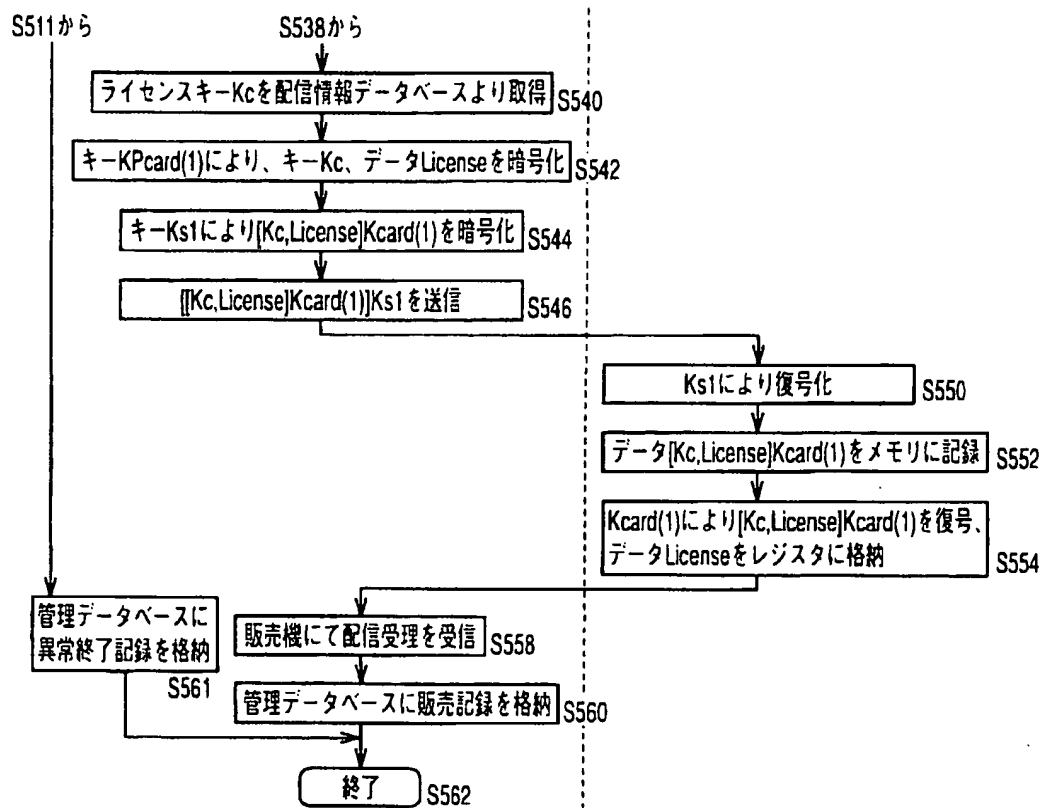


FIG.44

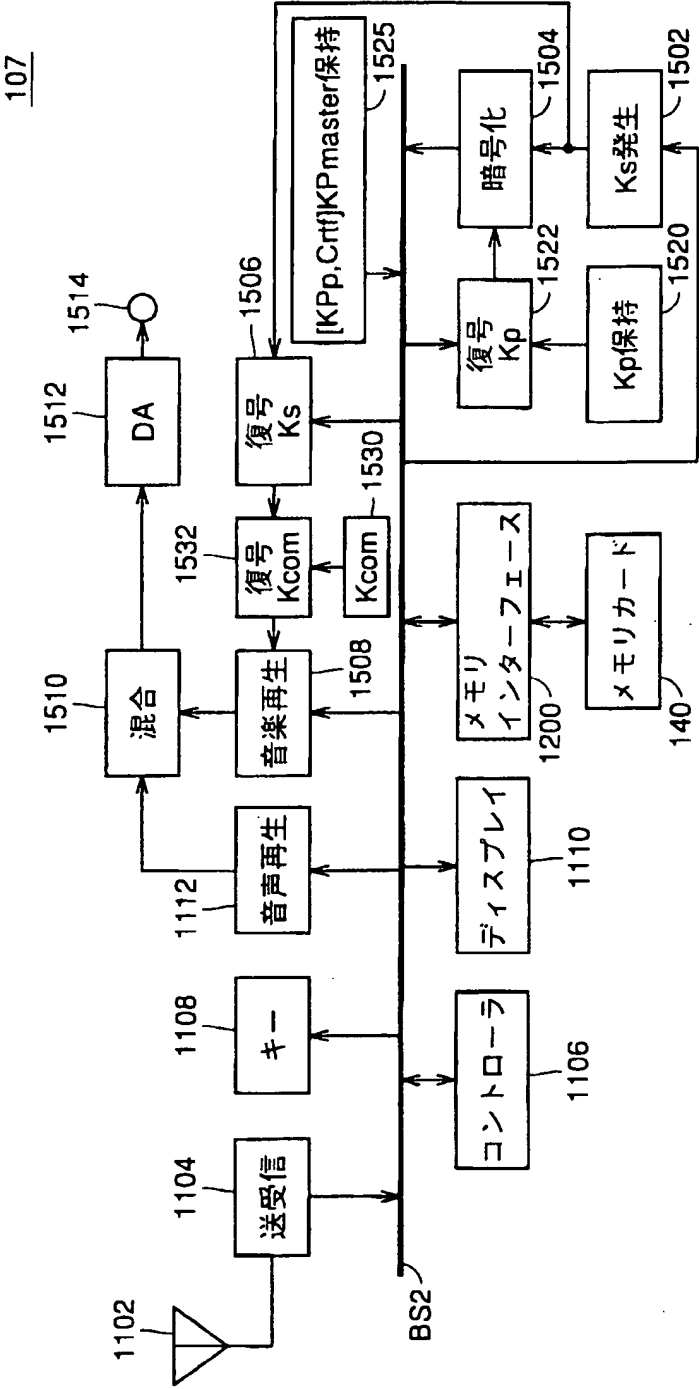


FIG.45

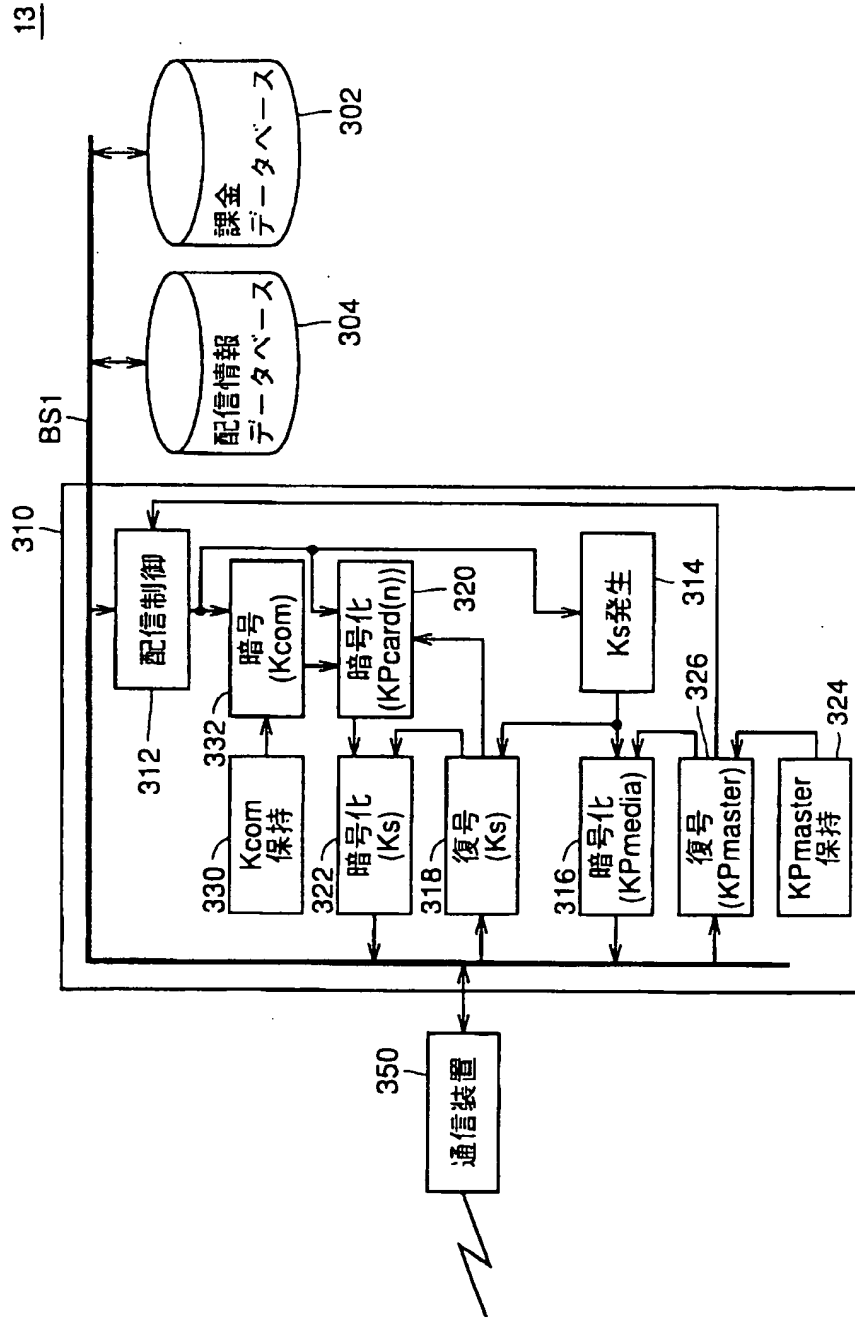


FIG. 46

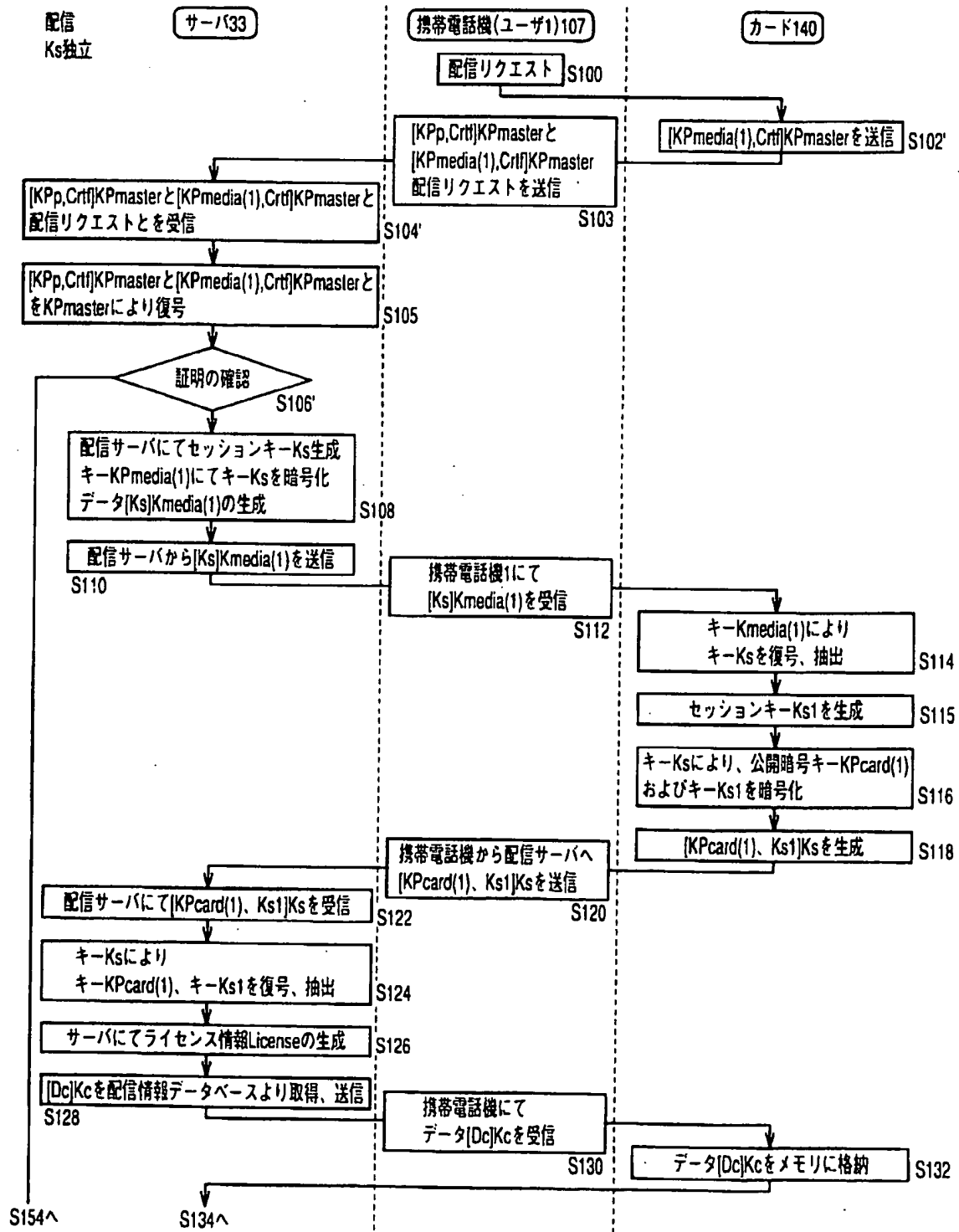


FIG. 47

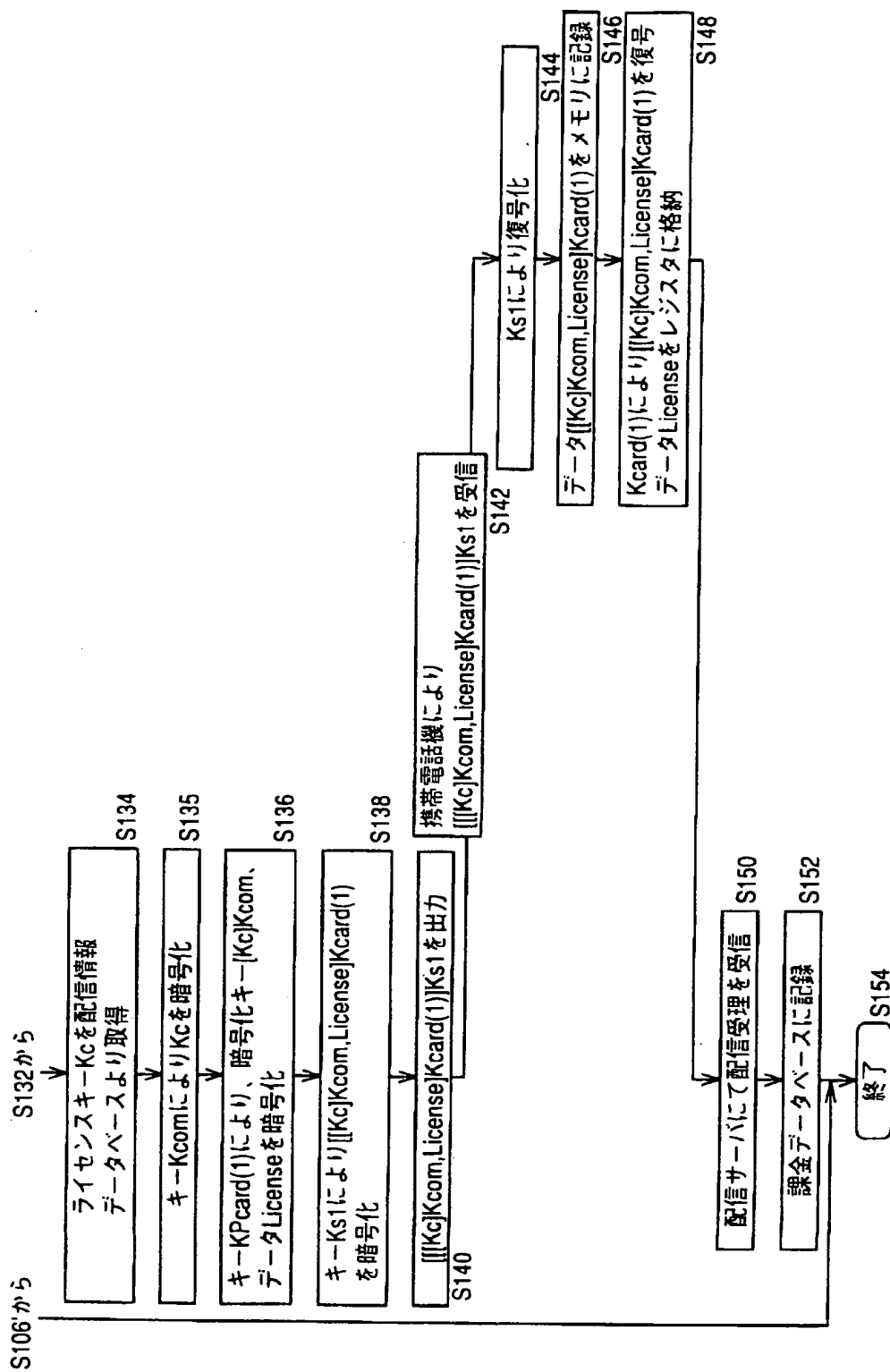




FIG. 48

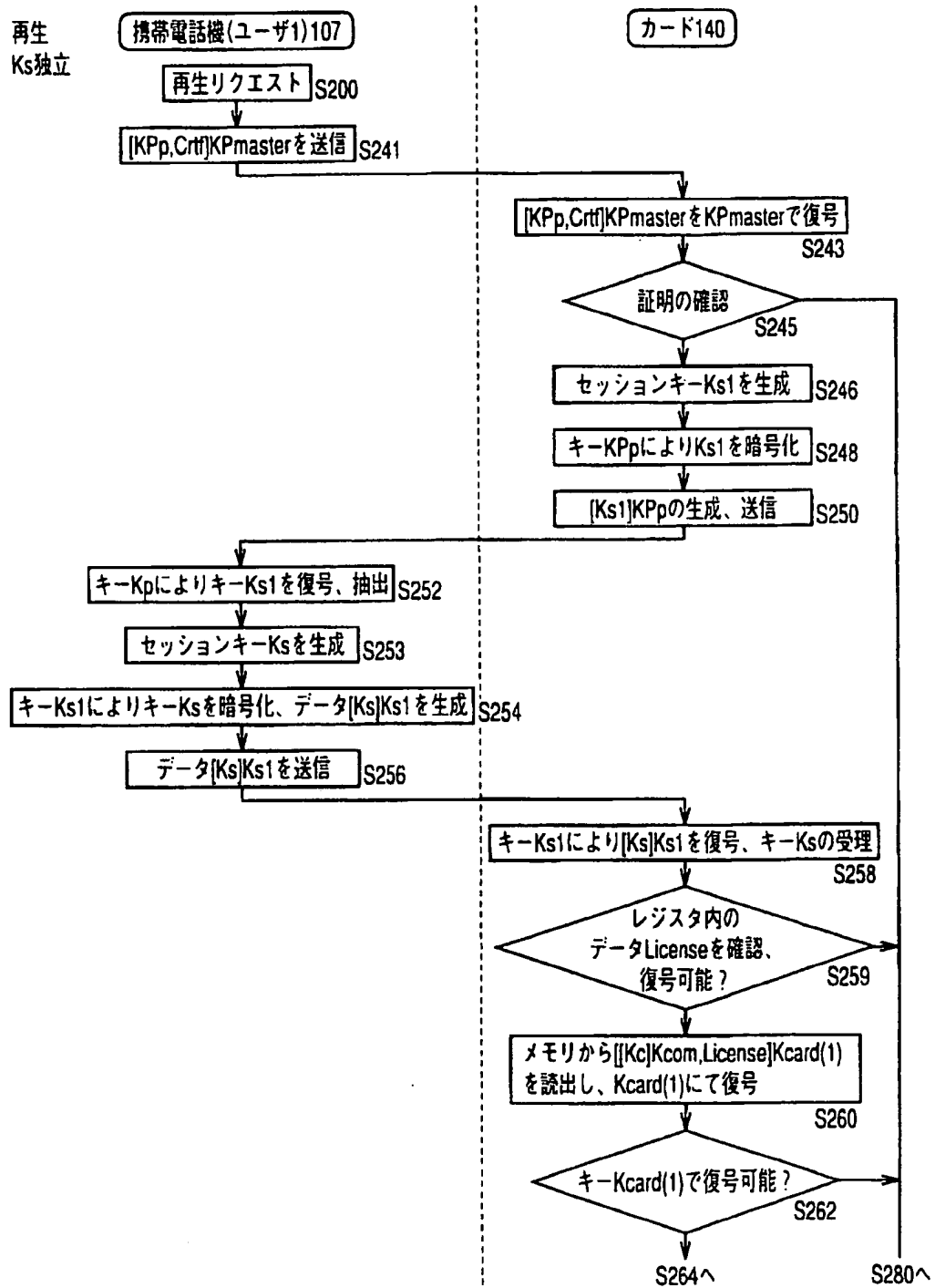
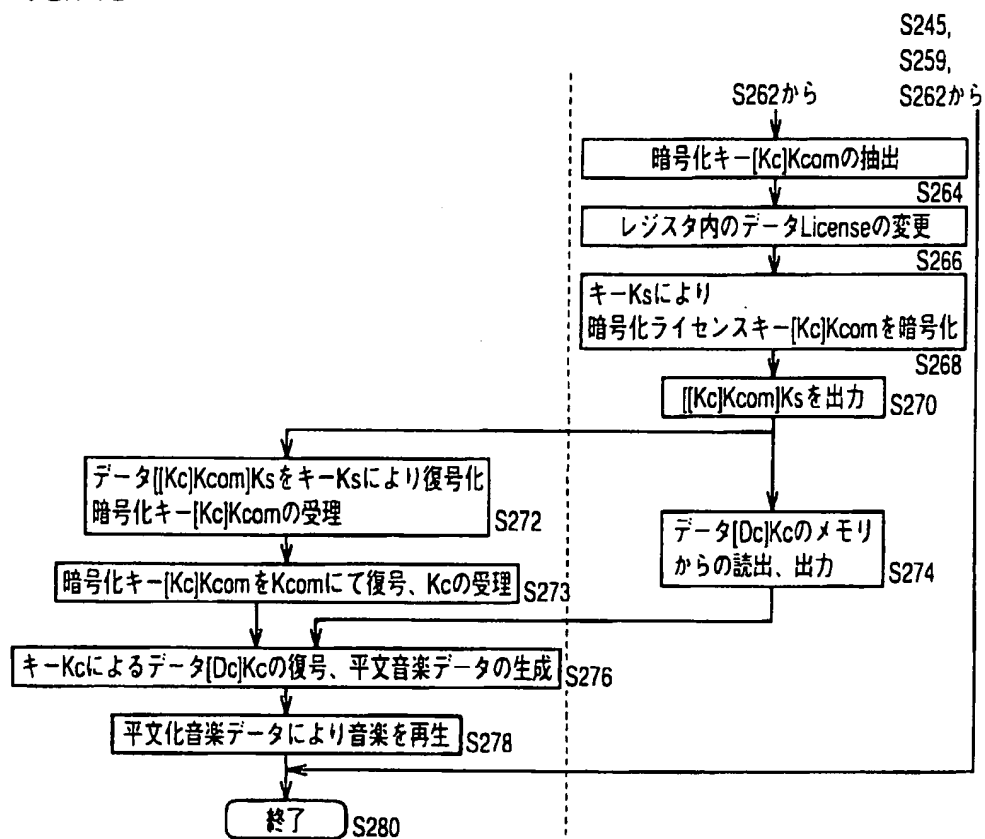


FIG. 49



**FIG. 50**

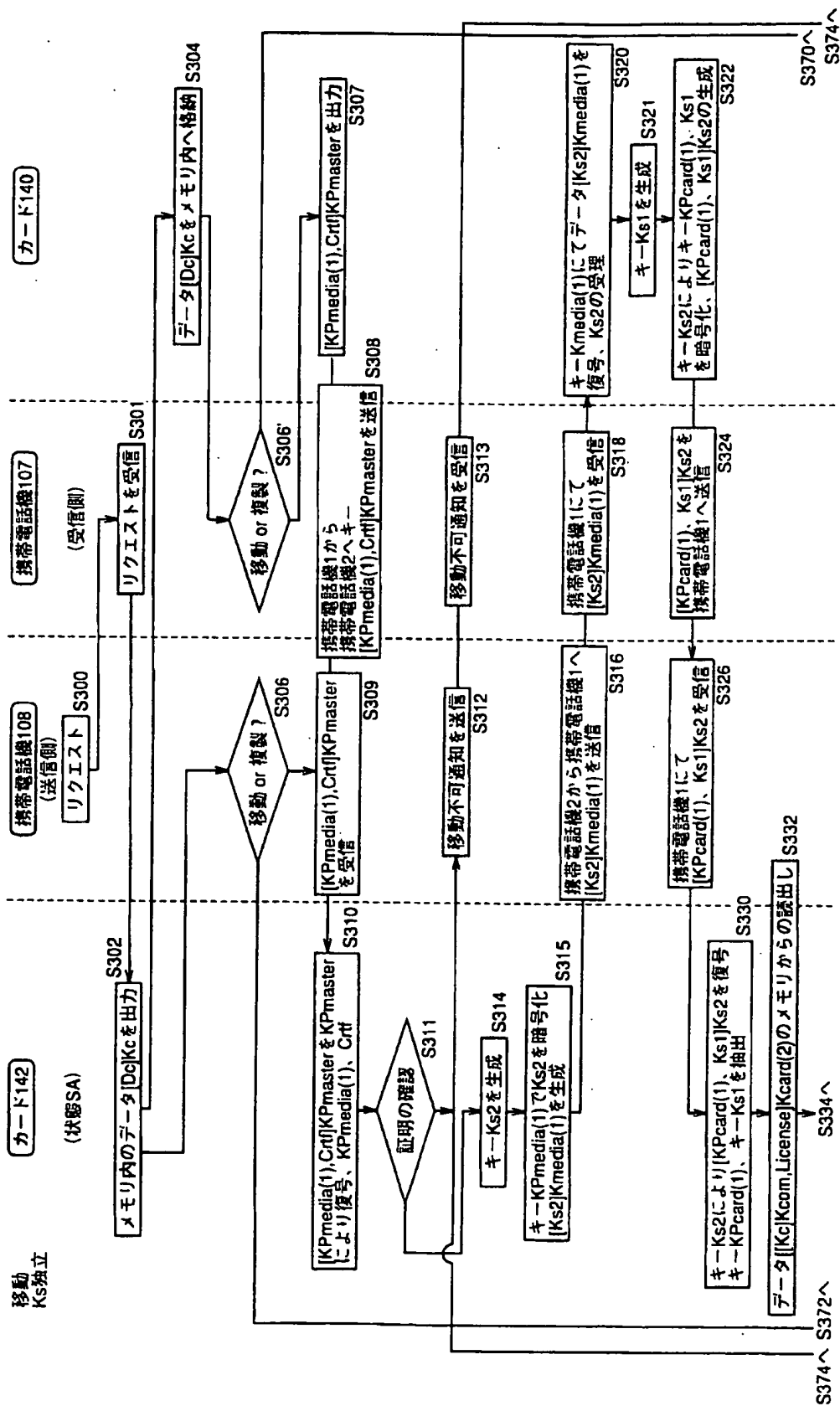


FIG.51

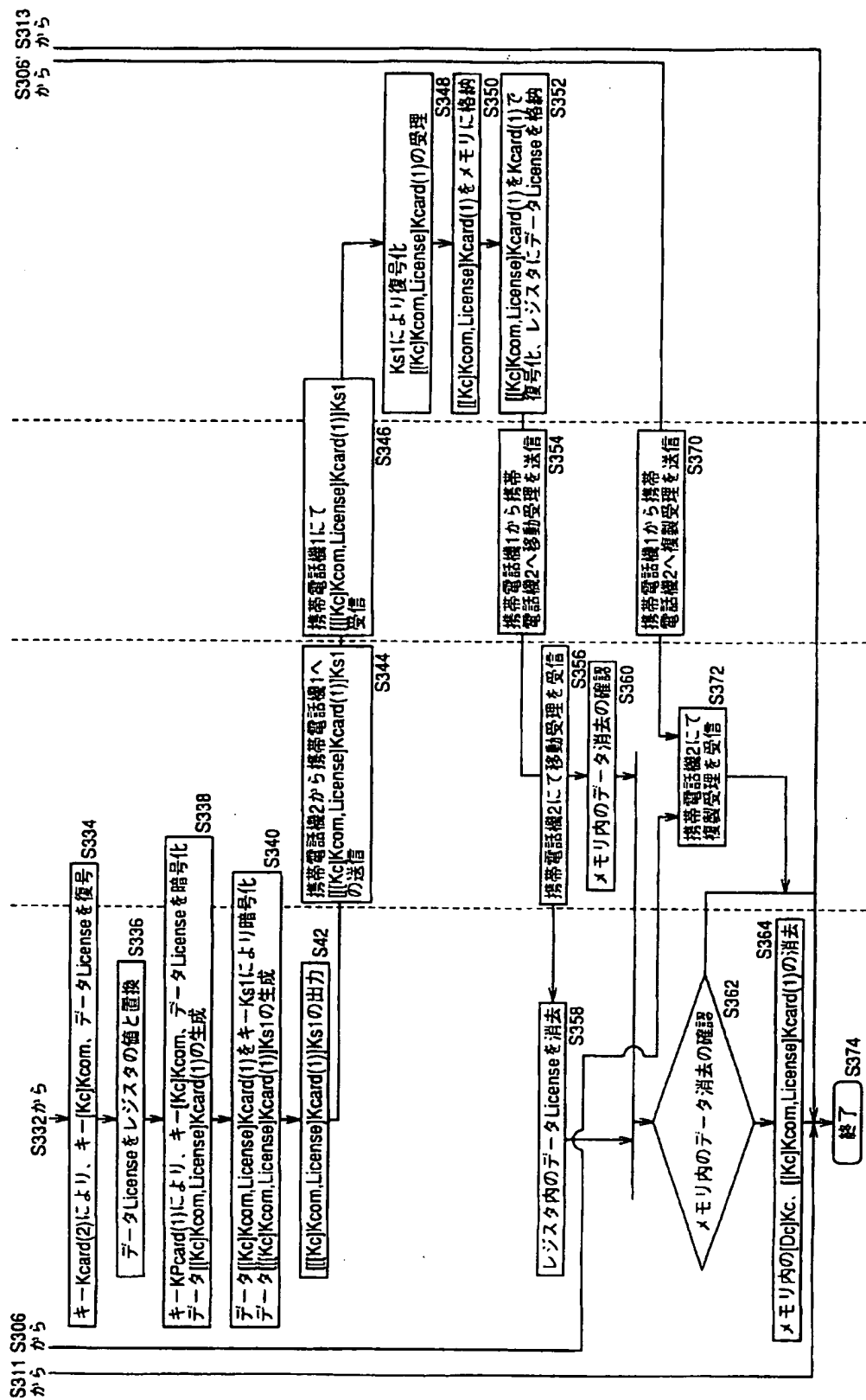


FIG.52

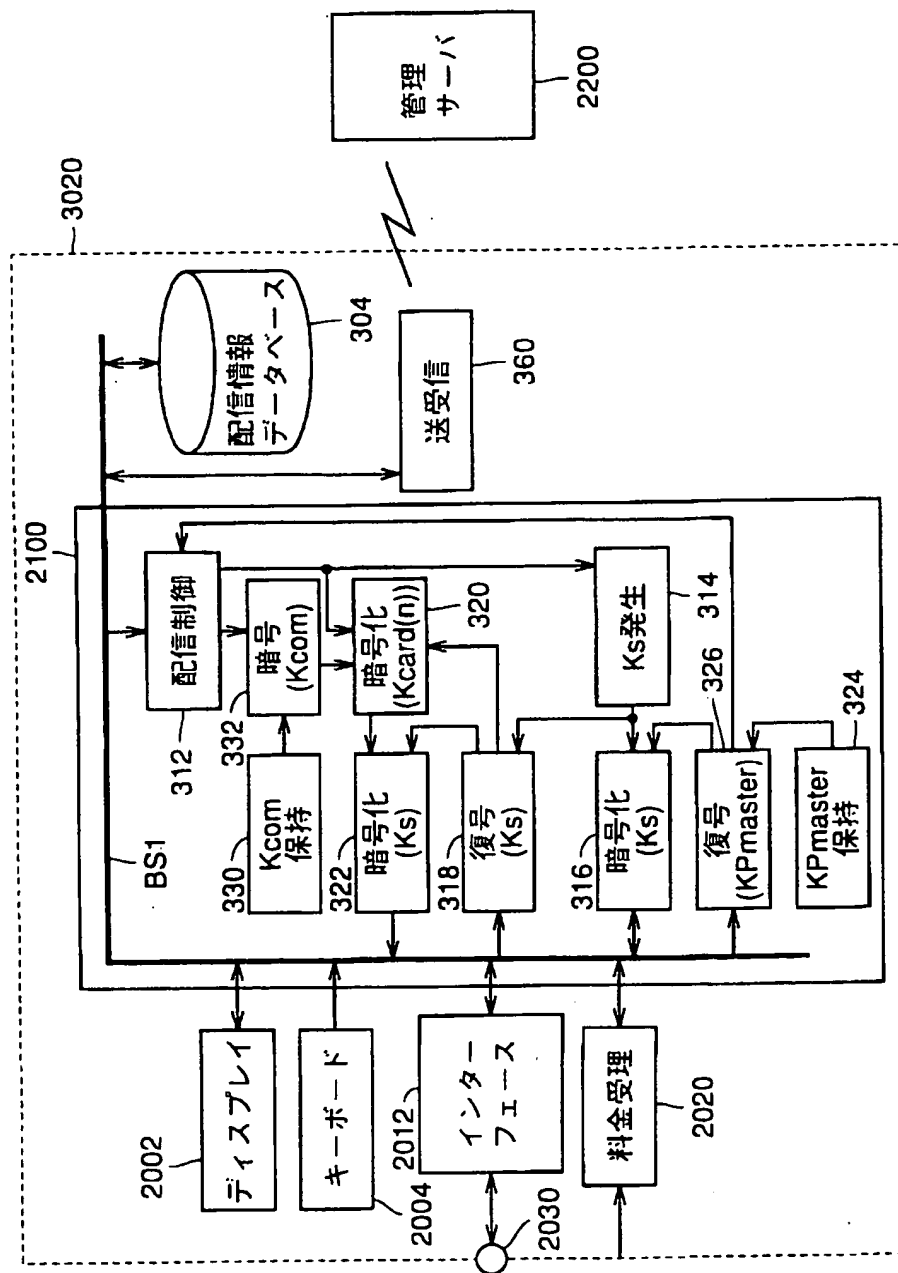


FIG.53

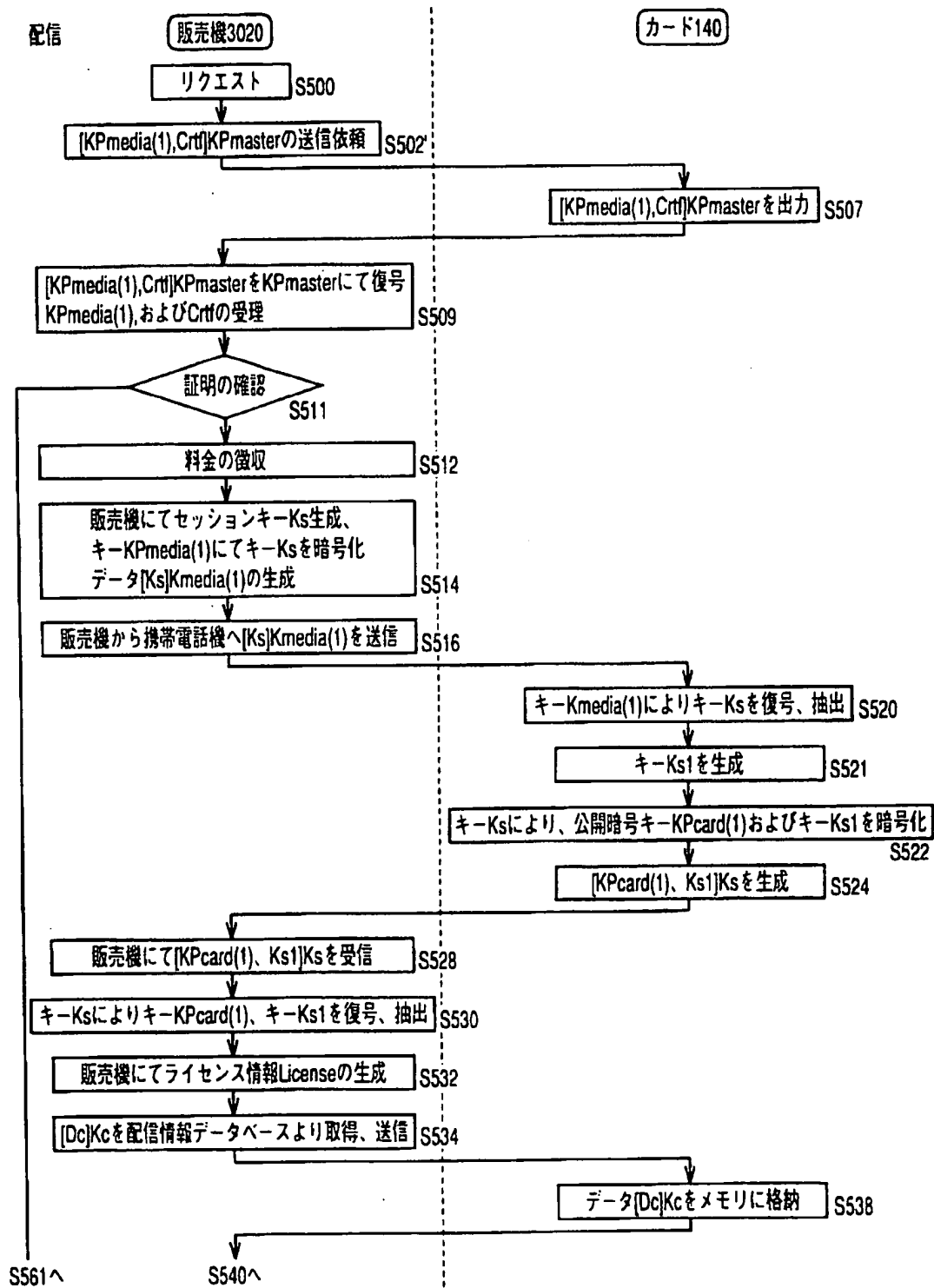


FIG.54

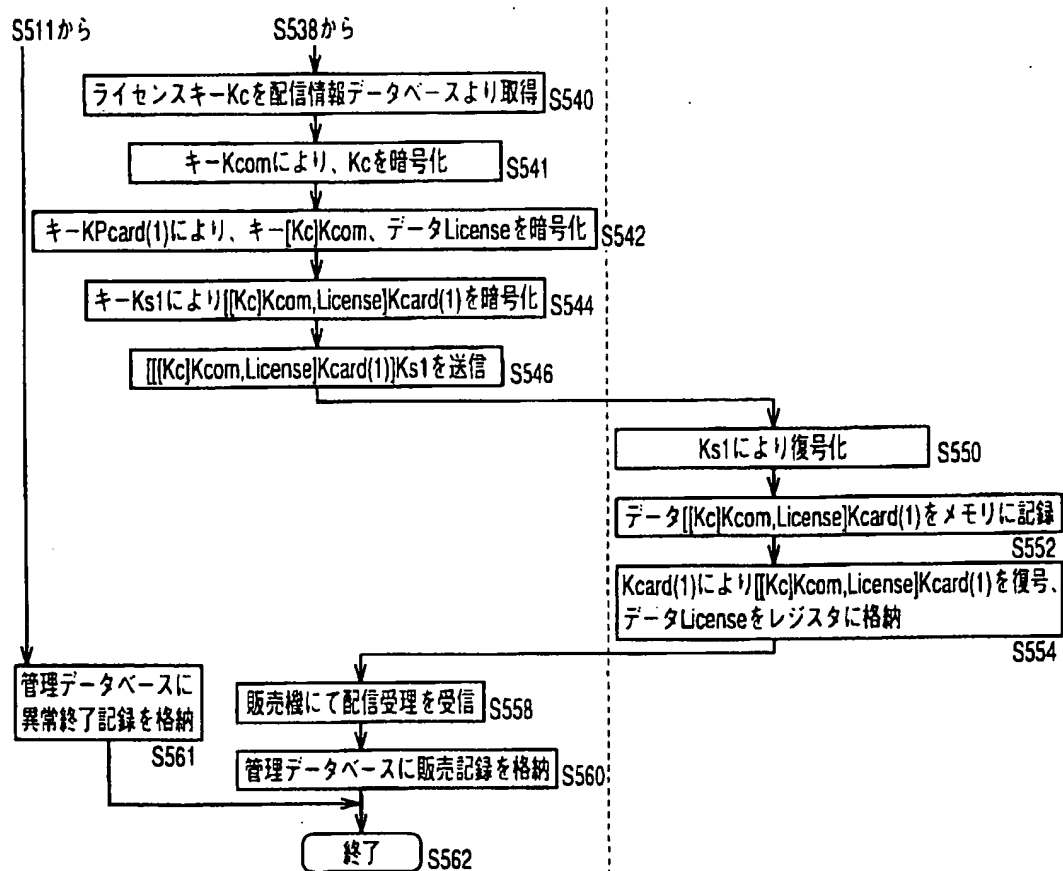


FIG.55

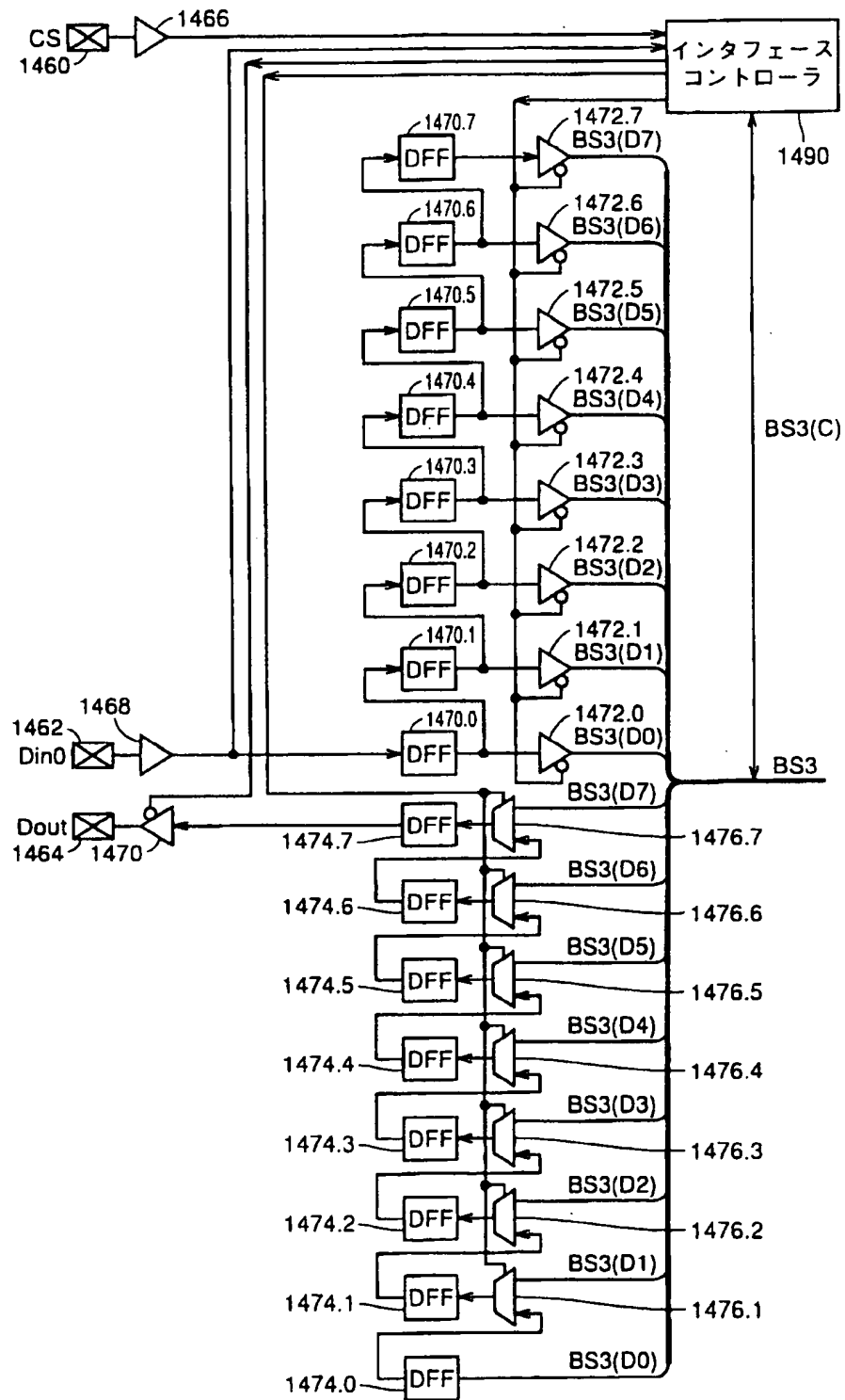
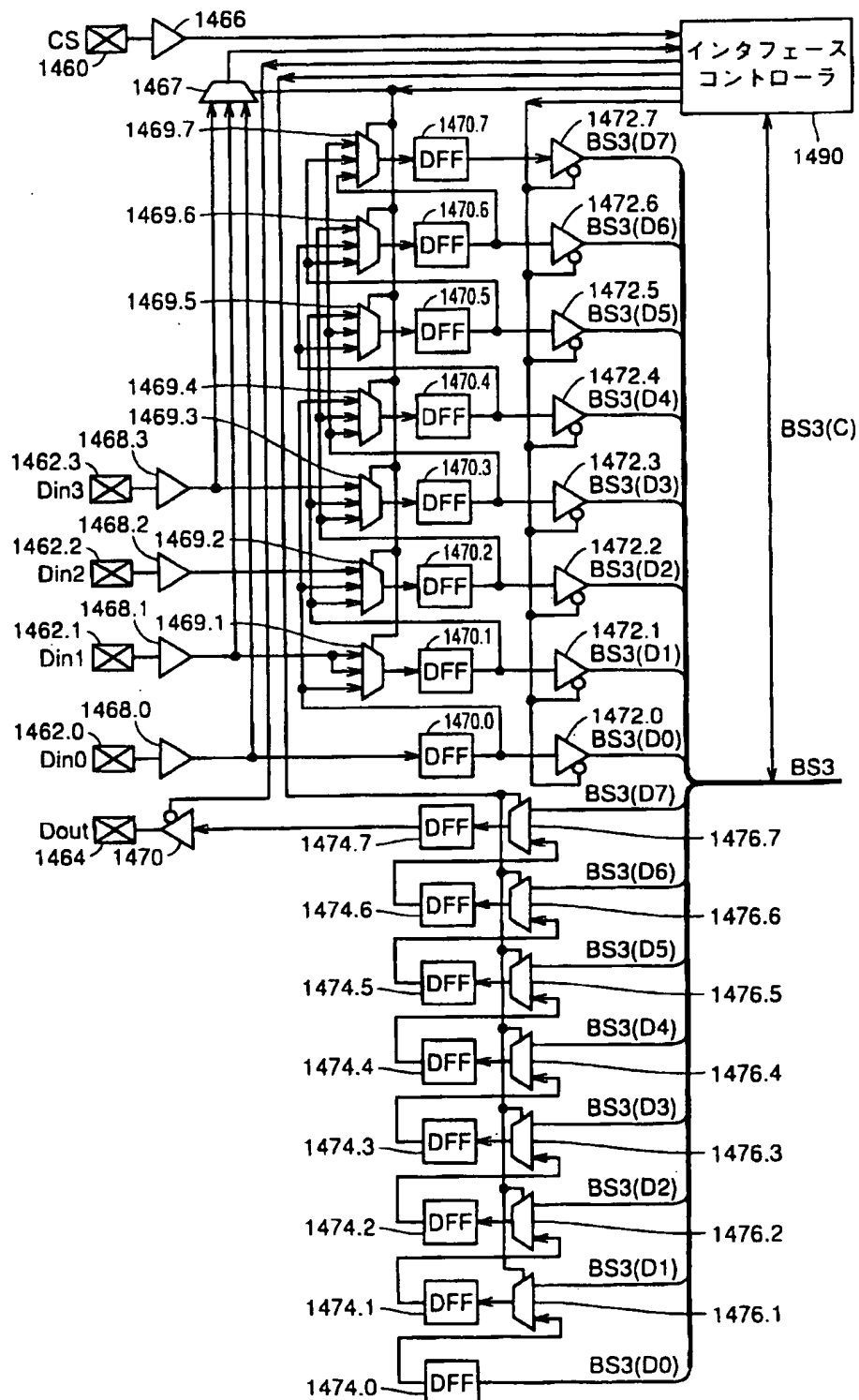




FIG.56



## INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP00/05770

## A. CLASSIFICATION OF SUBJECT MATTER

Int.Cl<sup>7</sup> G10K15/02, G06F15/00, G06F17/60, H04L9/08, H04L9/10,  
G06K19/00, H04H1/00, H04M3/42, H04M3/493, H04M11/08,  
G10L19/00, G06F13/00, H04L12/22, H04L12/58

According to International Patent Classification (IPC) or to both national classification and IPC

## B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int.Cl<sup>7</sup> G10K15/00~15/06, G10L19/00~19/14, H04L9/00~9/38,  
G09C1/00~5/00, G06F12/00, G06F12/14, G06K19/00,  
H04M11/00~11/08

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched  
Jitsuyo Shinan Koho 1926-1995 Toroku Jitsuyo Shinan Koho 1994-2000  
Kokai Jitsuyo Shinan Koho 1971-2000 Jitsuyo Shinan Toroku Koho 1996-2000

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)  
INSPEC (DIALOG)  
WPI (DIALOG)

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP, 561685, A2 (FUJITSU LIMITED), 22 September, 1993 (22.09.93), Full text, all drawings & US, 5392351, A & US, 5555304, A & US, 5796824, A & JP, 5-257816, A & JP, 3073590, B2	1-33
A	JP, 62-53042, A (Nippon Telegr. & Teleph. Corp. <NTT>), 07 March, 1987 (07.03.87), Full text, all drawings (Family: none)	1-33
A	JP, 8-186667, A (Matsushita Electric Ind. Co., Ltd.), 16 July, 1996 (16.07.96), Full text, all drawings (Family: none)	1-33
A	JP, 8-69419, A (Shimadzu Corporation), 12 March, 1996 (12.03.96), Full text, all drawings (Family: none)	1-33
E, A	JP, 11-328033, A (Fujitsu Limited), 30 November, 1999 (30.11.99), Full text, all drawings (Family: none)	1-33

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:	"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A" document defining the general state of the art which is not considered to be of particular relevance	"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E" earlier document but published on or after the international filing date	"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&" document member of the same patent family
"O" document referring to an oral disclosure, use, exhibition or other means	
"P" document published prior to the international filing date but later than the priority date claimed	

Date of the actual completion of the international search 10 November, 2000 (10.11.00)	Date of mailing of the international search report 21 November, 2000 (21.11.00)
Name and mailing address of the ISA/ Japanese Patent Office	Authorized officer
Facsimile No.	Telephone No.

## INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP00/05770

## C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	Nikkei Electronics, No.739, "Kogata Memory Card de Ongaku Chosakuken wo mamoru", 22 March, 1999 (22.03.99), pp.49-53	1-33
A	Nikkei Electronics, No.728, "Bei Shuuhun Kiki Maker Ootega, MP3 Keitei gata Player Hatsubai; Chosakuken Taisaku wa Tsuika sezu", 19 October, 1998 (19.10.98), pp.31-32	1-33
A	Nikkei Electronics, No.731, "Yogoreta Image Fusshoku nerau MP3 Gyoukai; Ongaku Haishin no Kaigi, 'Web noise' kara", 30 November, 1998 (30.11.98), pp.29-30	1-33

## 国際調査報告

国際出願番号 PCT/JPO0/05770

## A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int Cl<sup>i</sup> G10K15/02, G06F15/00, G06F17/60, H04L9/08, H04L9/10,  
G06K19/00, H04H1/00, H04M3/42, H04M3/493, H04M11/08,  
G10L19/00, G06F13/00, H04L12/22, H04L12/58

## B. 調査を行った分野

## 調査を行った最小限資料 (国際特許分類 (IPC))

Int Cl<sup>i</sup> G10K15/00~15/06, G10L19/00~19/14, H04L9/00~9/38,  
G09C1/00~5/00, G06F12/00, G06F12/14, G06K19/00,  
H04M11/00~11/08

## 最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報 1926~1995年  
日本国公開実用新案公報 1971~2000年  
日本国登録実用新案公報 1994~2000年  
日本国実用新案登録公報 1996~2000年

## 国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

INSPEC (DIALOG)  
WPI (DIALOG)

## C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
A	EP, 561685, A2 (FUJITSU LIMITED), 22.9月.1993(22.09.93), 全文全図, &US, 5392351, A &US, 5555304, A &US, 5796824, A &JP, 5-257816, A &JP, 3073590, B2	1-33
A	JP, 62-53042, A (日本電信電話株式会社), 7.3月.1987(07.03.87), 全文全図 (ファミリーなし)	1-33
A	JP, 8-186667, A (松下電器産業株式会社), 16.7月.1996(16.07.96), 全文全図 (ファミリーなし)	1-33

☒ C欄の続きにも文献が列挙されている。☐ パテントファミリーに関する別紙を参照。

## \* 引用文献のカテゴリー

「A」特に関連のある文献ではなく、一般的技術水準を示すもの

「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの

「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)

「O」口頭による開示、使用、展示等に言及する文献

「P」国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの

「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの

「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの

「&amp;」同一パテントファミリー文献

国際調査を完了した日

10.11.00

国際調査報告の発送日

21.11.00

国際調査機関の名称及びあて先

日本国特許庁 (ISA/JP)

郵便番号 100-8915

東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

松尾 淳一

印

5C

8842

電話番号 03-3581-1101 内線 3540

C (続き) . 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
A	J P, 8-69419, A (株式会社島津製作所), 12.3月.1996(12.03.96), 全文全図(ファミリーなし)	1-33
E, A	J P, 11-328033, A (富士通株式会社), 30.11月.1999(30.11.99), 全文全図(ファミリーなし)	1-33
A	日経エレクトロニクス, No.739, 「小型メモリ・カードで音楽著作権を守る」, 22.3月.1999(22.03.99), p.49-53	1-33
A	日経エレクトロニクス, No.728, 「米周辺機器メーカー大手が, MP3携帯型プレーヤ発売 著作権対策は付加せず」, 19.10月.1998(19.10.98), p.31-32	1-33
A	日経エレクトロニクス, No.731, 「汚れたイメージ払拭ねらうMP3業界 音楽配信の会議 Webnoise から」, 30.11月.1998(30.11.98), p.29-30	1-33